ウェブサイトの攻撃兆候検出ツール
iLogScanner V4.0

取扱説明書
（オンライン版）

平成 26 年 10 月

独立行政法人
情報処理推進機構

目次

1. はじめに 1
1.1. このプログラムの目的 1
1.2. 機能概要 1
1.3. 解析対象の攻撃 1
1.3.1. アクセスログ、エラーログから検出できるウェブアプリケーション脆弱性 .. 2
1.3.2. 認証ログから検出できる項目 4
1.4. 攻撃の痕跡の検出条件 6
1.4.1. アクセスログ、エラーログ 6
1.4.2. 認証ログ 9
2. 動作環境について 11
2.1. 動作環境 11
2.2. ウェブブラウザの設定 11
2.3. Java の設定 12
2.4. アプレットへの署名確認 13
2.5. 解析対象ログファイル 14
2.5.1. アクセスログファイル形式 14
2.5.2. エラーログファイル形式 18
2.5.3. 認証ログファイル形式 20
3. 操作方法 23
3.1. アクセスログ解析機能の操作方法 23
3.1.1. 初期画面表示 23
3.1.2. アクセスログファイルの設定 24
3.1.3. 解析結果出力の設定 26
3.1.4. 詳細設定 28
3.1.5. 解析開始 32
3.1.6. 解析終了 33
3.1.7. 解析結果レポート 35
3.2. ModSecurity ログ解析機能の操作方法 38
3.2.1. 初期画面表示 38
3.2.2. 解析対象ファイルの指定 39
3.2.3. 解析結果出力の設定 40
3.2.4. 詳細設定 40
3.2.5. 解析開始 45
3.2.6. 解析終了 48

3.2.7. 解析結果レポート 49
3.2.8. ログ統計情報レポート出力機能 53
3.3. 認証ログ解析機能の操作方法 59
3.3.1. 初期画面表示 60
3.3.2. 解析対象ファイルの指定 61
3.3.3. 解析結果出力の設定 61
3.3.4. 詳細設定 61
3.3.5. 解析開始 68
3.3.6. 解析終了 69
3.3.7. 解析結果レポート 70
4. トラブルシュート 72
5. 付録 XML 形式の解析結果レポートファイル 73
5.1. XML スキーマ定義方針 73
5.2. XML スキーマ定義 73
5.3. XML 文書構造の全体像 74
5.4. 各種要素 75
5.5. 検出内容の対応コード（DetectionId） 82

1. はじめに

1.1. このプログラムの目的

IPA では、ウェブサイトに対してどれほどの攻撃を受けているのか、ウェブサイト管理者が簡単に状況を把握できる手段を提供していく必要があると考えています。そこで、ウェブサイトのアクセスログを解析することで、そのサイトへの攻撃痕跡を確認でき、一部の痕跡に関しては攻撃が成功した可能性を確認できるツール「iLogScanner」を開発しました。ウェブサイトへの攻撃が成功した可能性が確認された場合は、ウェブアプリケーションに潜む脆弱性を確認する事ができるとともに、インターネットに公開しているウェブサイトがどれほど危険であるかを認知してもらい、ウェブサイト管理者や経営者に対して警告を発し、対策を講じるきっかけとなる事が期待できます。

1.2. 機能概要

iLogScanner は、利用者がウェブブラウザを利用して IPA のウェブサイトからダウンロードし､利用者のウェブブラウザ上で実行するJavaアプレット形式のプログラムです。

iLogScanner は、利用者が用意したログファイルを解析し、ウェブサイトへの攻撃の有無およびログイン状況に関する解析結果をレポートとして出力します。解析対象のログファイルは以下の通りです。

・ウェブサーバ（Apache、IIS）のアクセスログ
・ウェブサーバ（Apache）のエラーログ(ModSecurity の出力にも対応)
・sshd、vsftpd の認証ログ

1.3. 解析対象の攻撃

iLogScanner で、アクセスログおよびエラーログから検出できるウェブアプリケーション攻撃の痕跡、および認証ログから検出できる項目は以下の通りです（2014 年 08 月現在)。

【ウェブアプリケーション攻撃の痕跡と攻撃が成功した可能性】

- SQL インジェクション

【ウェブアプリケーション攻撃の痕跡】

- OS コマンド・インジェクション
- ディレクトリ・トラバーサル
- クロスサイト・スクリプティング

- その他（IDS*回避を目的とした攻撃）

【詳細レベルの検出対象】

- 同一 IP アドレスから同一 URL に対する攻撃の可能性
- アクセスログに記録されない SQL インジェクションの兆候
- Web サーバの設定不備を狙った攻撃の可能性

【SSH、FTP に対する攻撃の痕跡】

- 大量のログイン失敗
- 短時間の集中ログイン
- 同一ファイルへの大量アクセス

【ユーザのログイン状況】

- 認証試行回数
- 業務時間外アクセス
- ルート昇格
- 指定 IP 外からのアクセス
- 特権アカウントでのログイン検知
- 長時間ログインの検知
- 匿名アカウントでのログイン検知
- ゲストアカウントでのログイン検知

1.3.1. アクセスログ、エラーログから検出できるウェブアプリケーション脆弱性

・ 「SQL インジェクション」とは

データベースと連携したウェブアプリケーションに問い合わせ命令文の組み立て方法に問題があるとき、ウェブアプリケーションへ宛てた要求に悪意を持って細工された SQL 文を埋め込まれて（Injection）しまうと、データベースを不正に操作されてしまう問題です。これにより、ウェブサイトは重要情報などが盗まれたり、情報が書き換えられたりといった被害を受けてしまう場合があります。

・ 「OS コマンド・インジェクション」とは

ウェブサーバ上の任意の OS コマンドが実行されてしまう問題です。これにより、ウェブサーバを不正に操作され、重要情報などが盗まれたり、攻撃の踏み台に悪用される場合があります。

・ 「ディレクトリ・トラバーサル」とは、

* IDS：侵入検知システム（Intrusion Detection System）

相対パス記法を利用して、管理者が意図していないウェブサーバ上のファイルやディレクトリにアクセスされたり、アプリケーションを実行される問題です。これらにより、本来公開を意図しないファイルが読み出され、重要情報が盗まれたり、不正にアプリケーションを実行されファイルが破壊されるなどの危険があります。

・ 「クロスサイト・スクリプティング」とは

ウェブサイトの訪問者の入力をそのまま画面に表示する掲示板などが、悪意あるスクリプト（命令）を訪問者のブラウザに送ってしまう問題です。これにより、アンケート、掲示板、サイト内検索など、ユーザからの入力内容をウェブページに表示するウェブアプリケーションで、適切なセキュリティ対策がされていない場合、悪意を持ったスクリプト（命令）を埋め込まれてしまい、ウェブページを表示した訪問者のプラウザ環境でスクリプトが実行されてしまう可能性があります。その結果として、cookie などの情報の漏洩や意図しないページの参照が行われてしまいます。

・ 「その他（IDS 回避を目的とした攻撃)」とは

１６進コード、親パス等の特殊文字を使用して偽装した攻撃用文字列で攻撃が行われることによりアプリケーションの妥当性チェック機構を迂回し、SQL インジェクション、クロスサイト・スクリプティング等の攻撃を行うことを狙ったものです。また、ワームなどが悪用するウェブサーバの脆弱性を突いた攻撃でも、このような特殊文字が使われます。それぞれの攻撃に応じた対策が必要になります。

・ 同一 IP アドレスからの攻撃の可能性

同一の IP アドレスからの攻撃痕跡（SQL インジェクション、OS コマンド・インジェクション等）が一定件数に達しています。基準値を超えているため、攻撃を受けている可能性があります。

・ アクセスログに記録されない SQL インジェクションの兆候
ウェブサーバが「SQL インジェクション」の攻撃の影響を受けている可能性を示すものです。同一 IP アドレスから行われたリクエストに対するウェブサーバからのエラー応答が、基準値に達しています。

・ Web サーバの設定不備を狙った攻撃の可能性
Web サーバの設定不備を狙った攻撃を受けている可能性があります。
対象となる設定不備は以下の通りです。
「PUT メソッドの設定不備」
「FrontPage Server Extensions の設定不備」
「Tomcat の設定不備」

脆弱性については、IPA　セキュリティセンターの「知っていますか？脆弱性（ぜいじゃくせい）」http://www.ipa.go.jp/security/vuln/vuln_contents/index.html で解説が行われていますので、ご参照ください。

1.3.2. 認証ログから検出できる項目

・ 大量のログイン失敗
一定時間内に、**同一のユーザ ID** で閾値を越える大量のログイン失敗があったことを検出します。パスワードを総当りで入力するなどの手段で不正アクセスを試みられている可能性があります。

・ 短時間の集中ログイン
一定時間内に閾値を越える大量のログイン要求があったことを検出します。同一のパスワードでユーザ ID を総当りで入力するなどの手段で不正アクセスを試みられている可能性や、サーバリソースに負荷をかける目的で大量アクセスが行われている可能性があります。

・ 同一ファイルへの大量アクセス
一定時間内に同一のファイルに対する大量のアクセスがあったことを検出します。サーバリソースに負荷をかける目的で大量アクセスが行われている可能性があります。

・ 認証試行回数
総認証試行回数、成功数、失敗数を集計します。試行回数が通常時と比べて極端に多い場合、攻撃を受けている可能性があります。

・ 業務時間外アクセス
業務時間外のアクセスを検出します。通常アクセスが行われない時間帯にアクセスがあった場合、サーバを不正に利用しようとしている可能性があります。

・ ルート昇格
ルートに昇格しようとしたユーザとその成否を検出します。許可されていないユーザがルート昇格を試みている場合、サーバを不正に利用しようとしている可能性があります。

・ 指定 IP 外からのアクセス
指定した範囲外の IP アドレスからのアクセスを検出します。通常利用されない IP アドレスからのアクセスがあった場合、サーバに不正アクセスが試みられている可能性があります。

・ 特権アカウントでのログイン検知
特権アカウント（ルート）でログインしたユーザを検出します。特権アカウントで直接ログインすることはセキュリティ上好ましくないため、特権アカウントでのログインを無効にすることをご検討ください。

・ 長時間ログインの検知
長時間ログイン状態のユーザを検出します。極端に長時間ログイン状態のユーザが存在する場合、不正アクセスの踏み台などに使用されている可能性があります。

・ 匿名アカウントでのログイン検知
匿名アカウントでのログインを検出します。匿名アカウントの利用はセキュリティ上好ましくないため、匿名アカウントを無効にすることをご検討ください。

・ ゲストアカウントでのログイン検知
ゲストアカウントでのログインを検出します。ゲストアカウントが適正に管理されており、ゲストアカウントでのログインが正当なものかどうかをご確認ください。

1.4. 攻撃の痕跡の検出条件

1.4.1. アクセスログ、エラーログ

ウェブサーバのアクセスログに記録されたリクエストのクエリ文字列から、ウェブアプリケーションへの攻撃によく見られる文字列が存在した場合に検出しています。
それぞれの攻撃でよく見られる文字列は次のような意味のある文字列になります。

攻撃種別	文字列
SQL インジェクション	・ SQL ステートメントで使用されるキーワード ・ データベースのシステムテーブル名 ・ SQL ステートメントで使用される関数 ・ システムストアドプロシージャ名 ・ システム拡張ストアドプロシージャ名
OS コマンド・インジェクション	コンピュータの基本ソフトウェアを操作するための命令文やそれらのパラメータ文
ディレクトリ・トラバーサル	ディレクトリ操作文
クロスサイト・スクリプティング	・ スクリプト関数 ・ HTML タグ文字列 ・ イベントハンドラ
その他（IDS*回避を目的とした攻撃）	特殊文字を使用して、偽装した文字列

- 一般的な GET メソッドを使用したウェブアプリケーションについて、リクエストのクエリ文字列から攻撃と思われる痕跡を検出しています。
- 一般的な POST メソッドを使用したウェブアプリケーションについては、リクエストのクエリ文字列がアクセスログに出力されないため、攻撃と思われる痕跡を iLogScanner で検出することはできません。
- ウェブアプリケーションへ無差別に攻撃するような一部の攻撃は、POST メソッドによる攻撃の場合でもリクエストのクエリ文字列がアクセスログに出力される場合があるため、iLogScanner で検出できる場合があります。
- 攻撃が成功した可能性が高いかどうかを検出することができるのは、SQL インジェクションの攻撃と思われる痕跡からのみとなります。

* IDS：侵入検知システム（Intrusion Detection System）

オプション選択画面で解析レベルの詳細を選択した場合、以下 3 項目による解析を行っています。これらは、以下の基準値や条件を設定し、その基準値を超えた場合や条件を満たした場合に攻撃の可能性があると判断しています。また、一部ではウェブサーバのアクセスログに記録されたリクエストのクエリ文字列から、ウェブアプリケーションへの攻撃によく見られる文字列が存在した場合に検出する方法をとっています。

- 同一 IP アドレスから同一 URL に対する攻撃の可能性

攻撃検出用シグネチャによる解析結果に対して、以下の基準にて、再解析を行います。表中の条件を全て満たす場合、攻撃と判断します。

No.	攻撃判定の条件
条件 1	同一 IP アドレスから同一 URL（CGI、ASP、JSP 等を含むウェブアプリケーション全般）に対する攻撃痕跡が一定件数に達している
条件 2	同一 IP アドレスからの攻撃痕跡が一定件数に達している

※標準解析による脆弱性 5 種類の分類は問いません。

- アクセスログに記録されない SQL インジェクションの兆候

アクセスログに次の表中の条件を全て満たすリクエストが記録されている場合、ログに記録されないタイプの SQL インジェクション攻撃が行われた可能性があると判断します。

No.	攻撃判定の条件
条件 1	アクセスログに記録されたリクエストの応答コード （サーバレスポンス）が 5xx 番台であること かつ POST メソッドであること
条件 2	条件 1 に合致するリクエストが ・同一 IP アドレスにより ・一定時間以内に規定数回以上行われている

- Web サーバの設定不備を狙った攻撃の可能性

No.	対象	判断基準
1	PUT メソッドの設定不備	リクエストのメソッドが PUT であり、リクエストに対する応答コードが 201 であること
2	FrontPage Server Extensions の設定不備	FrontPage Server Extensions の設定不備を狙うような、特定ファイル URL に対するリクエストが行われていること
3	Tomcat の設定不備	Tomcat の設定不備を狙うような、特定ファイル（URL）に対するリクエストが行われていること

1.4.2. 認証ログ

認証ログの解析では、SSH、FTP のログに記録された認証情報や認証結果、ファイルへのアクセス回数をカウントし、検出項目の条件に当てはまるものがあるか調べています。それぞれの検出項目の検出条件は以下の通りです。

検出項目	検出条件
大量のログイン失敗	基準時間内の同一ユーザ名によるログイン試行回数が基準値に達した場合
短時間の集中ログイン	基準時間内のログイン試行回数が基準値に達した場合
同一ファイルへの大量アクセス検知	基準時間内に同一のファイル名に対するファイルアクセス（ダウンロード）が基準値に達した場合
認証試行回数	ログに含まれるログイン試行総回数
業務時間外アクセス	ログイン時の時間が指定された業務時間外だった場合
ルート昇格	ルート昇格の操作が行われた場合
指定 IP 外からのアクセス	ログイン時の接続元 IP アドレスが指定範囲外だった場合
特権アカウントでのログイン検知	ログイン時のユーザ名が root だった場合
長時間ログインの検知	ログイン～ログアウトの時間差が基準値を超えていた場合
匿名アカウントでのログイン検知	ログイン時のユーザ名が anonymous または ftp だった場合
ゲストアカウントでのログイン検知	ゲストユーザでのログインだった場合

なお、認証ログの種類によって検出可能な項目が異なります。ログの種類と検出可能な項目の対応は以下の通りです。

認証ログ / 検出項目	sshd (syslog)	vsftpd (vsftpd 形式)	vsftpd (wu-ftpd 形式)
大量のログイン失敗	○	○	—
短時間の集中ログイン	○	○	—
同一ファイルへの大量アクセス検知	—	○	○
認証試行回数	○	○	—
業務時間外アクセス	○	○	○
ルート昇格	○	—	—
指定 IP 外からのアクセス	○	○	○
特権アカウントでのログイン検知	○	○	○
長時間ログインの検知	○	—	—
匿名アカウントでのログイン検知	—	○	○
ゲストアカウントでのログイン検知	—	—	○

2. 動作環境について

2.1. 動作環境

iLogScanner が動作する環境は、以下を想定しています。

CPU	Intel Pentium4 2.8GHz 以上を推奨
搭載メモリ	1GB 以上を推奨
オペレーティングシステム	Microsoft Windows Vista (32bit) Microsoft Windows 7 (32bit / 64bit) Microsoft Windows 8 (32bit / 64bit) Microsoft Windows 8.1 (32bit / 64bit)
ウェブブラウザ	Internet Explorer 8 以上
Java 実行環境（JRE）	Java Runtime Environment(JRE) 6.0 以上

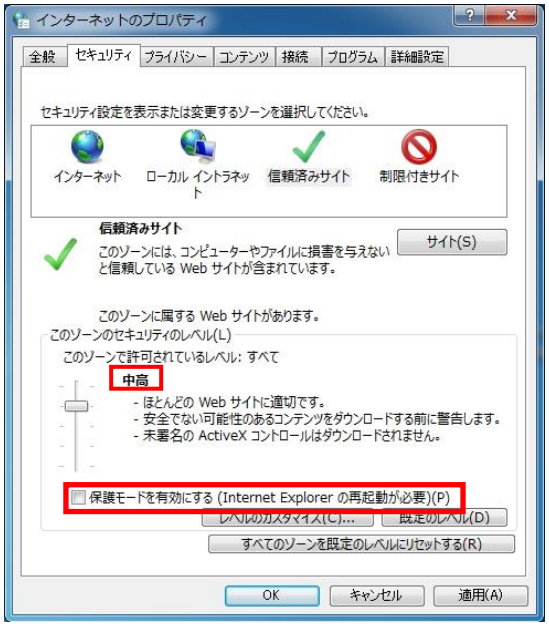
2.2. ウェブブラウザの設定

Java アプレットである iLogScanner を実行するために、ウェブブラウザ（Internet Explorer）で次の設定を行ってください。設定を変更した場合は、Internet Explorer を再起動して設定を反映させる必要があります。

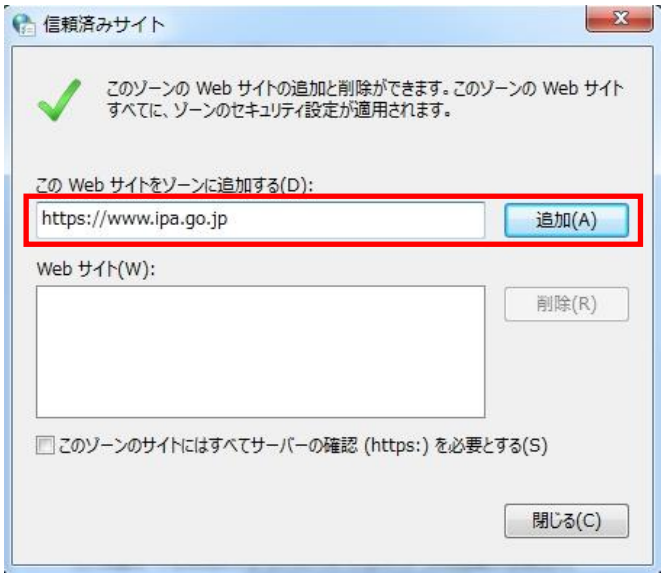
(1) 「インターネットオプション」の「セキュリティ」タブを開き、『信頼済みサイト』ゾーンが以下の設定になっていることを確認してください。

・「このゾーンのセキュリティのレベル」:『中高』または『中』

・「保護モードを有効にする」のチェックなし



(2) 「サイト」ボタンをクリックし、https://www.ipa.go.jp を信頼済みサイトに追加してください。

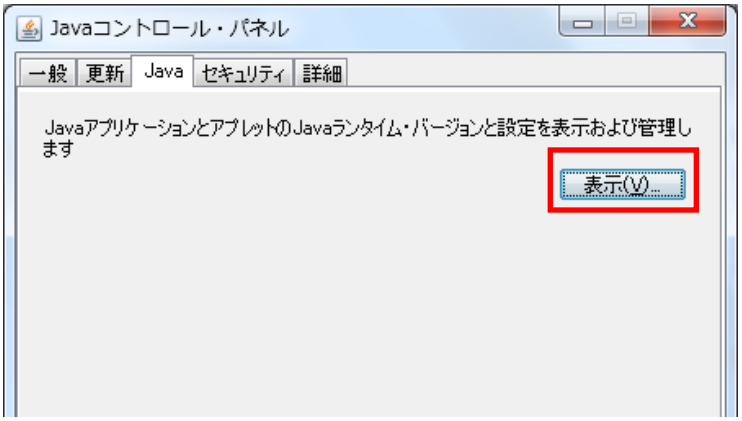


2.3. Java の設定

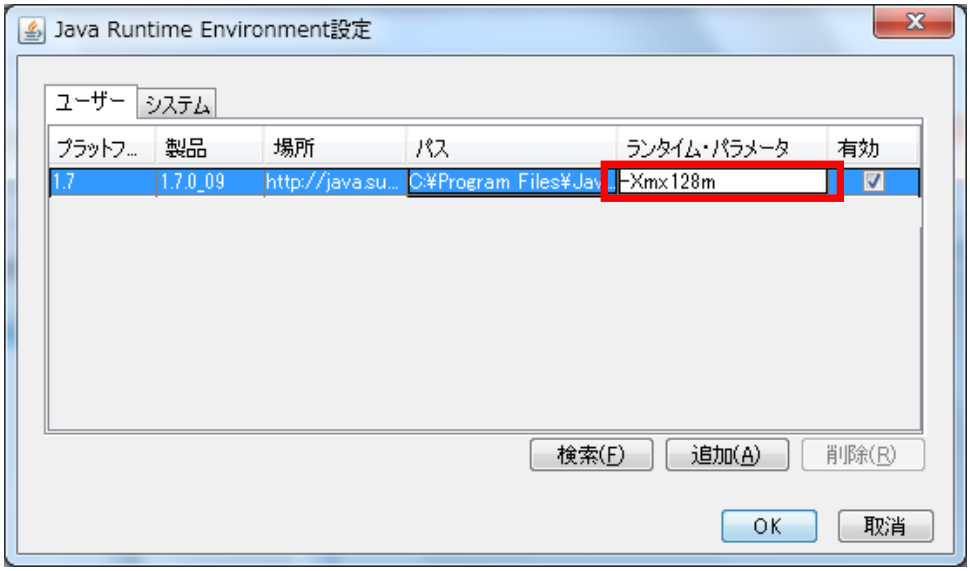
Java に関する設定は、特に必要ありません。

iLogScanner 実行中に、「メモリが不足しています」という旨のエラーメッセージが表示され処理が中止された場合は、次の設定で Java が使用するメモリの最大サイズを大きくしてください（デフォルトでは 64MB です）。

(1) コントロールパネルの「Java」より「Java コントロールパネル」を開きます。「Java 」タブの「表示」ボタンをクリックし、「Java ランタイム設定」画面を開きます。



(2)　「Java ランタイム設定」画面の「Java ランタイムパラメータ」に「-Xmx(size)m」を入力します（下記画像の例は 128MB の場合）。何も入力しない場合（デフォルト）、Java が使用するメモリの最大サイズは 64MB です。



2.4.　アプレットへの署名確認

iLogScanner は電子署名された Java アプレット形式のプログラムです。このため、iLogScanner 実行時に、実行されるアプレットを信頼するかどうかのセキュリティ警告画面が表示されます。

セキュリティ警告画面では、「名前、発行者、ダウンロード元」を確認し、このアプレットが IPA から提供されていることを確認してください。詳細情報を確認する場合は、「証明書の詳細」をクリックし、発行者が信頼される機関であることと有効期限が切れていないことを確認してください。電子署名を確認後は、実行ボタンを押して iLogScanner を実行してください。

注意：セキュリティ警告画面にて実行ボタンが押されなかった場合、iLogScanner は動作しません。

2.5. 解析対象ログファイル

2.5.1. アクセスログファイル形式

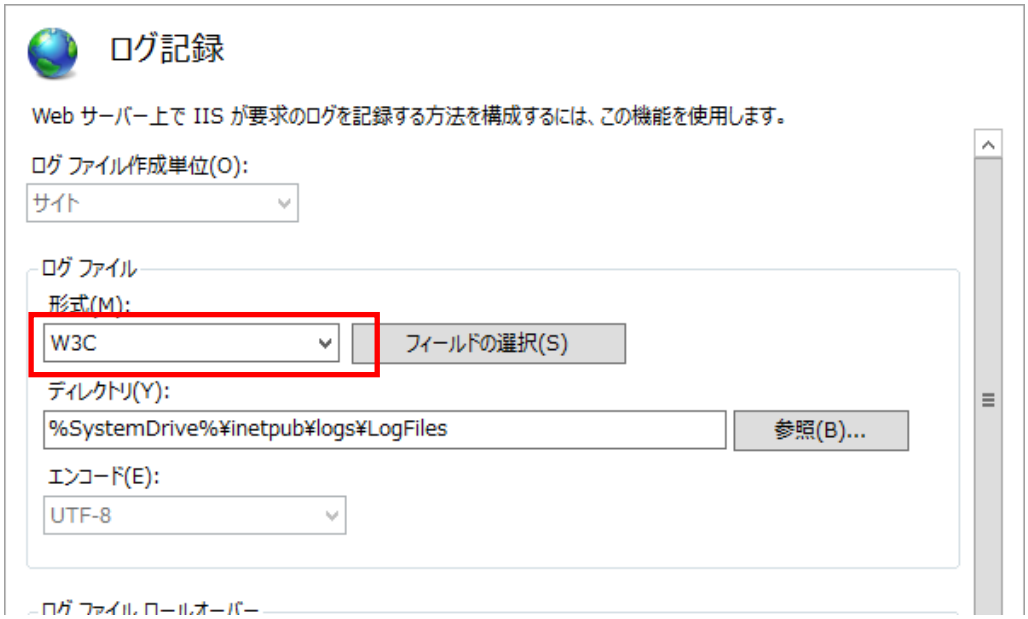
iLogScanner は以下のウェブサーバソフトウェアのアクセスログフォーマットに対応しています。

ウェブサーバソフトウェア	プラットフォーム	アクセスログフォーマット
Microsoft インターネット インフォメーション サービス(IIS 6.0、7.0、7.5、8.0、8.5)	Windows	W3C 拡張ログファイル形式
		IIS ログファイル形式
Apache HTTP Server(1.3 系、2.0 系、2.2 系、2.4 系)	Windows、Linux	Common Log Format

iLogScanner では、アクセスログに出力された GET メソッドのクエリ文字列を解析します。POST メソッドはアクセスログにクエリ文字列が出力されないため、POST メソッドを使用したウェブアプリケーションへの攻撃痕跡の検出には対応していません。

(1) W3C 拡張ログファイル形式

「インターネット インフォメーション サービス (IIS) マネージャ」の Web サイトの「ログ記録」において、ログファイルの形式が「W3C」になっている必要があります。



（画面は、IIS8.0 のプロパティになります）

また、フィールドの選択オプションにおいて次の必須項目が有効になっている必要があります。

■必須項目

日付(date)
時間(time)
クライアント IP アドレス(c-ip)
ユーザ名(cs-username)
サーバ IP アドレス(s-ip)
サーバポート(s-port)
メソッド(cs-method)
URI Stem(cs-uri-stem)
URI クエリ(cs-uri-query)
プロトコルの状態(sc-status)
ユーザエージェント(cs(User-Agent))

(2)　IIS ログファイル形式

「インターネット インフォメーション サービス (IIS) マネージャ」の Web サイトの「ログ記録」において、ログファイルの形式が「IIS」になっている必要があります。

（画面は、IIS8.0 のプロパティになります）

以下は IIS6.0/7.0/7.5/8.0/8.5 の IIS ログファイル形式のログ項目一覧です。

■IIS6.0/7.0/7.5/8.0/8.5 の IIS ログ項目一覧

クライアント IP アドレス
ユーザ名
要求日付
要求時刻
サービス名
サーバ IP アドレス
処理時間
受信バイト数
送信バイト数
サービス状態コード
システム状態コード
メソッド
URI Stem
URI クエリ

(3) Common Log Format

Apache HTTP Server の設定で、Common Log Format（デフォルトで定義されているニックネーム「common」形式）のアクセスログが出力されている必要があります。また、先頭からの書式が Common Log Format と同じ Combined Log Format（デフォルトで定義されているニックネーム「combined」形式）であれば解析することが可能です。

■Apache HTTP Server のアクセスログ出力設定例

```
LogFormat "%h %l %u %t ¥"%r¥" %>s %b" common
CustomLog logs/access_log common
```

■Apache HTTP Server の Common Log Format(CLF)書式

フォーマット文字列	説明
%h	リモートホスト
%l	(identd からもし提供されていれば)リモートログ名
%u	リモートユーザ
%t	リクエストを受け付けた時刻。CLF の時刻の書式(標準の英語の書式)。
¥"%r¥"	リクエストの最初の行
%>s	最後のステータス
%b	レスポンスのバイト数。HTTP ヘッダは除く。CLF 書式。

(4) Apache アクセスログのフォーマット指定

Apache アクセスログのフォーマットが指定できます。そのため、記録項目および順序がカスタマイズされている Apache アクセスログを解析することができます。2.5.1(3)に記載されている CLF 書式の項目を必須項目と定義とします。また、各項目の区切り文字として「半角スペース」が設定されている必要があります。

入力例）LogFormat "%t %h %l %u ¥"%r¥" %>s %b" common

Apache HTTP Server に設定できる書式指定子（以下の「入力可能な書式指定子」に示す項目）のみ入力可能とします。

【入力可能な書式指定子】

%h %l %u %t %r %s %b %% %a %A %B %C %D
%e %f %i %m %n %o %p %P %q %T %U %v %V %X %I %O
%{Foobar}C %{Foobar}e %{Foobar}i %{Foobar}n %{Foobar}o

※ Foobar は、「任意の文字列」

2.5.2. エラーログファイル形式

iLogScanner は以下のウェブサーバソフトウェアのエラーログフォーマットに対応しております。

ウェブサーバソフトウェア	プラットフォーム	エラーログフォーマット
Apache HTTP Server(2.0 系、2.2 系)	Windows、Linux	ModSecurity2.5 系/2.6 系/2.7 系/2.8 系が出力するエラーログ形式
Apache HTTP Server(2.4 系)		

(1) ModSecurity2.5 系/2.6 系/2.7 系/2.8 系が出力するエラーログ形式

ModSecurity2.5系/2.6系/2.7系/2.8系が出力するApacheのエラーログ形式で、ModSecurity の設定で次の必須項目が有効になっている必要があります。

■必須項目

項目概要	例
アクセス日時	Sat Dec 12 11:20:50 2009
Apache のエラーレベル	error
アクセス元 IP アドレス	client 192.168.1.1
メッセージ	msg “SQL Injection Attack”
タグ	tag “WEB_ATTACK/SQL_INJECTION”
リクエスト URI	uri "/query.php"
リクエストの固有番号	unique_id "Sjr2An8AAAEAABJlx2kAAAAJ"

■ ModSecurity による Apache エラーログの出力例

```
[Sat Dec 12 11:20:50 2009] [error] [client 192.168.1.1] ModSecurity: Warning. Pattern match "(?:¥¥b(?:(?:s(?:elect¥¥b(?:.{1,100}?¥¥b(?:(?:length|count|top)¥¥b.{1,100}?¥¥bfrom|from¥¥b.{1,100}?¥¥bwhere)|.*?¥¥b(?:d(?:ump¥¥b.*¥¥bfrom|ata_type)|(?:to_(?:numbe|cha)|inst)r))|p_(?:(?:addextendedpro|sqlexe)c|(?:oacreat|prepar)e|execute(?:sql)?|makewebtask)|ql_(?...” at ARGS:id. [file "/usr/local/apache2/conf/modsec2/modsecurity_crs_40_generic_attacks.conf"] [line "66"] [id "950001"] [msg "SQL Injection Attack"] [data "or 1="] [severity "CRITICAL"] [tag "WEB_ATTACK/SQL_INJECTION"] [hostname "centos5.localdomain"] [uri "/query.php"] [unique_id "Sjr2An8AAAEAABJlx2kAAAAJ"]
```

(2) Apache エラーログのフォーマット指定

Apache HTTP Server 2.4 系をご利用の場合、エラーログのフォーマットが指定できます。フォーマットには以下の表の項目が出力されている必要があります。Apache HTTP Server の設定で設定できる書式指定子（以下の「入力可能な書式指定子」に示す項目）のみ入力可能とします。

【入力可能な書式指定子】

%% %a %{c}a %A %{Foobar}e %E %F %{Foobar}i %k %l %L %{c}L %{C}L %m %M %i %m %M %{Foobar}n %P %T %{g}T %t %{u}t %{cu}t %v %V ¥ %

※ Foobar は、「任意の文字列」

2.5.3. 認証ログファイル形式

iLogScanner は以下のサーバソフトウェアとログフォーマットに対応しております。

サーバソフトウェア	プラットフォーム	ログフォーマット	デフォルトの出力先
sshd	Linux	syslog	/var/log/secure ※ /var/log/messages
vsftpd		vsftpd 形式	/var/log/vsftpd.log
		wu-ftpd 形式	/var/log/xferlog

※OS のバージョンによりデフォルトの出力先が異なります

(1) 認証ログと検知可能な項目

認証ログファイルの形式によって検知可能な項目が異なります。ファイル形式と検知可能な項目は以下の通りです。

認証ログ / 検出項目	syslog	vsftpd 形式	wu-ftpd 形式
大量のログイン失敗	○	○	—
短時間の集中ログイン	○	○	—
同一ファイルへの大量アクセス検知	—	○	○
認証試行回数	○	○	—
業務時間外アクセス	○	○	○
ルート昇格	○	—	—
指定 IP 外からのアクセス	○	○	○
特権アカウントでのログイン検知	○	○	○
長時間ログインの検知	○	—	—
匿名アカウントでのログイン検知	—	○	○
ゲストアカウントでのログイン検知	—	—	○

(2) syslog

以下のいずれかの syslog 形式で出力されている必要があります。

テンプレート名	意味
RSYSLOG_TraditionalFileFormat	rsyslogd のデフォルトフォーマット（旧来の syslog 形式）
RSYSLOG_FileFormat	高精度タイムスタンプ、タイムゾーン情報を含む

※RSYSLOG_TraditionalFileFormat では、ログに年情報が含まれないため、一部の解析が正しく行われない場合があります
現在のテンプレートを確認するには、rsyslog.conf の
$ActionFileDefaultTemplate の値を確認します。
※未指定の場合は RSYSLOG_TraditionalFileFormat となります

(3) vsftpd 形式

vsftpd 形式のログは、設定により出力先を任意のログファイルまたは syslog から選択できます。iLogScanner で解析を行う場合は、vsftpd 形式のログをログファイルに出力する必要があります。

以下は vsftpd 形式のログ項目一覧です。

■vsftpd 形式のログ項目一覧

出力日時
プロセス ID
ユーザ名
処理結果
処理名
リモート IP アドレス
パスワード
詳細メッセージ
ファイルサイズ
転送レート

vsftpd.conf の設定が以下の値になっている場合、vsftpd 形式のログが出力されます。

・xferlog_enable=YES　かつ xferlog_std_format=NO　かつ
syslog_enable=NO
・xferlog_enable=YES　かつ dual_log_enable=YES　かつ syslog_enable=NO

(4) wu-ftpd 形式

以下は wu-ftpd 形式のログ項目一覧です。

■wu-ftpd 形式のログ項目一覧

出力日時
転送にかかった時間
リモートホスト名
ファイルサイズ
転送されたファイル名
転送の種類
特殊な操作が行われたことを示す文字
転送の方向
ユーザ種別
ユーザ名
サービス名
認証メソッド
認証メソッドにより復帰したユーザ名
転送状態

vsftpd.conf の設定が以下の値になっている場合、wu-ftpd 形式のログが出力されます。

・xferlog_enable=YES　かつ xferlog_std_format=YES

・xferlog_enable=YES　かつ dual_log_enable=YES

3. 操作方法

3.1. アクセスログ解析機能の操作方法

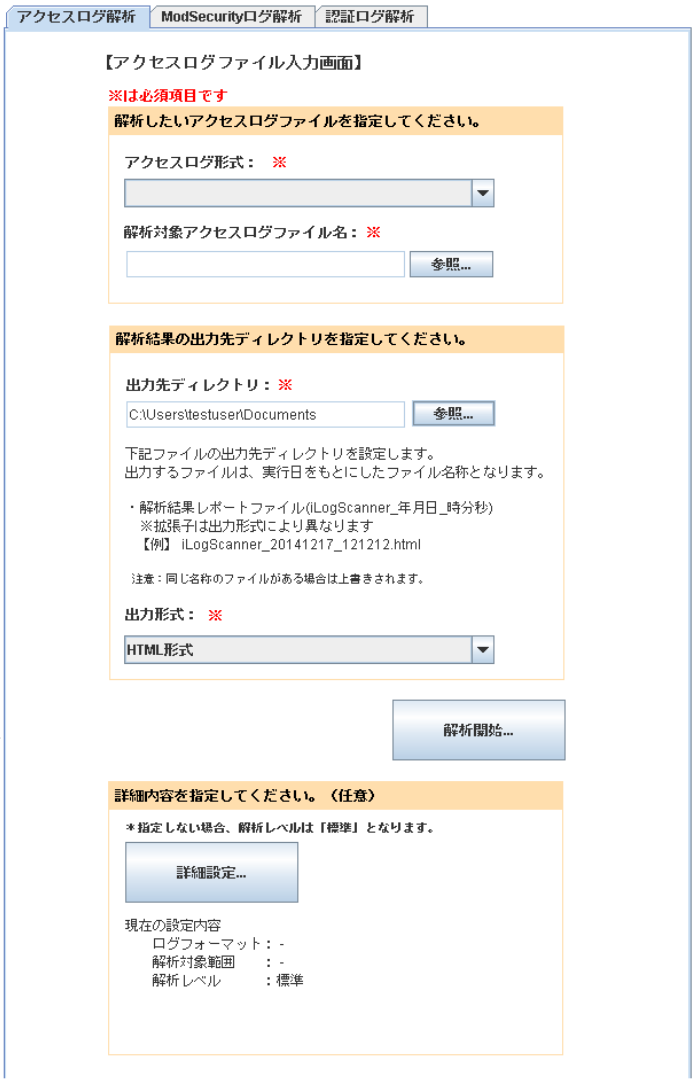
iLogScanner は、指定したアクセスログの解析を行い、解析結果を出力します。

アクセスログ解析のために必要な項目を入力し、解析を実行すると、解析実行中画面が表示され、進捗状況を確認することができます。アクセスログ解析後は、解析結果ファイルを作成し、結果画面が表示されます。

3.1.1. 初期画面表示

iLogScanner トップページで、オンライン版 iLogScanner の利用許諾内容を確認し、利用許諾に同意される方は「利用許諾に同意する」をチェックして「オンライン版 iLog Scanner を起動する」ボタンを押して下さい。iLogScanner が起動し、初期画面が表示されます。

「利用許諾に同意する」をチェックしていない場合、iLogScanner は起動しません。



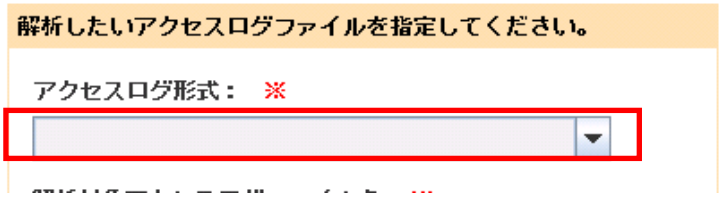
3.1.2. アクセスログファイルの設定

解析を行うアクセスログファイルの形式と解析対象ファイルを指定します。

アクセスログについては、「2.5　アクセスログファイル形式」を参照してください。

(1)　アクセスログファイル形式選択

解析を行うアクセスログファイルのファイル形式をプルダウンで選択します。

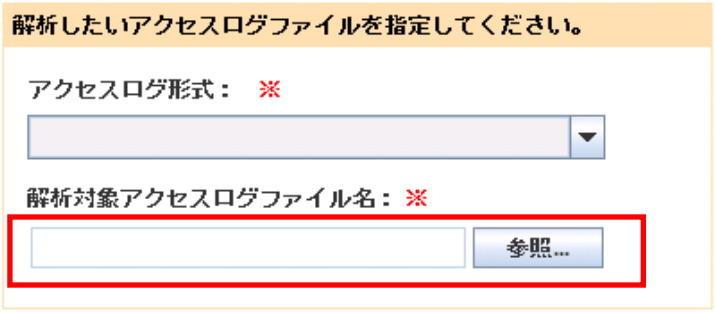


選択可能な形式は以下の通りです。

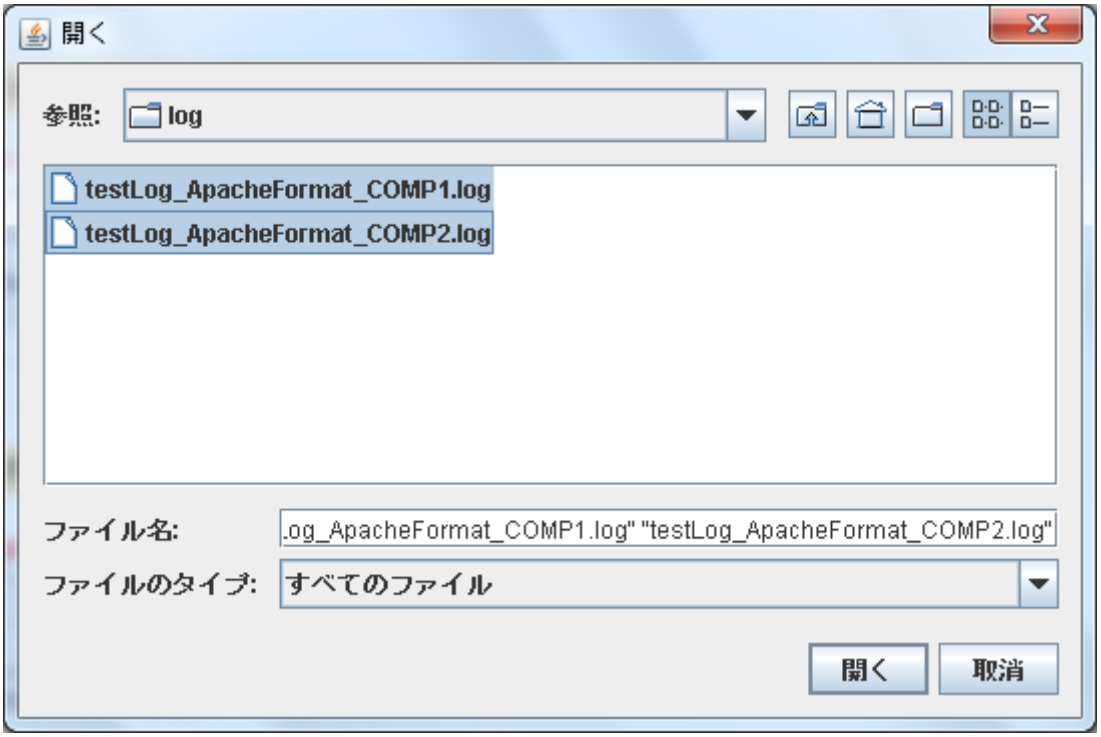
・IIS6.0/7.0/7.5/8.0/8.5 の W3C 拡張ログファイルタイプ
・IIS6.0/7.0/7.5/8.0/8.5 の IIS ログファイルタイプ
・Apache1.3 系/2.0 系/2.2 系/2.4 系の common タイプ

(2)　解析対象アクセスログファイル名選択

「参照」ボタンを押すと、ファイル選択画面が表示されます。



ファイル選択画面にて解析を行うアクセスログファイル名を選択し、開くボタンを押してください。また、アクセスログファイルは複数選択することも可能です。複数選択する場合は、Shift キー(または Ctrl キー)を押しながらファイルを選択します。



3.1.3. 解析結果出力の設定

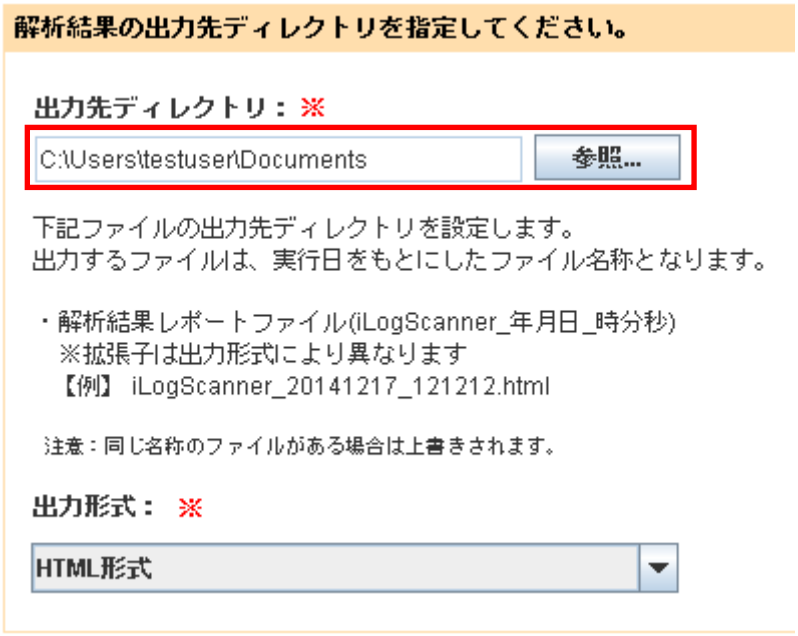
解析結果レポートの出力先と形式を指定します。

(1) 出力先ディレクトリ選択

解析結果を出力するディレクトリを指定します。初期値は Windows の場合ユーザ配下の Documents ディレクトリ、Linux の場合ユーザのホームディレクトリです。

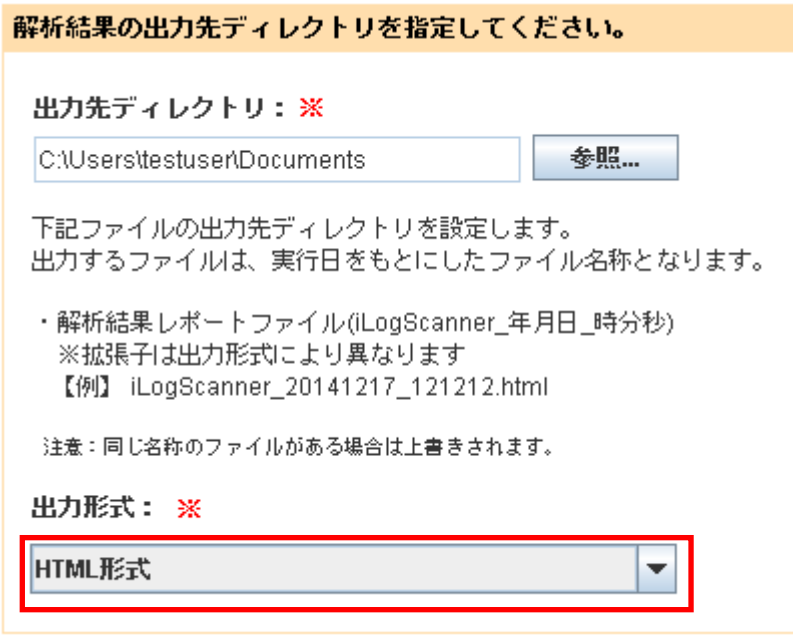
参照ボタンを押すと、ディレクトリ選択画面が表示されます。ディレクトリ選択画面にて、解析結果レポートファイルの出力先を選択します。解析結果レポートファイルについては「3.1.7 解析結果レポート」を参照して下さい。

エラー時に出力するエラーログもここで設定したディレクトリに出力されます。出力ディレクトリ設定前にエラーが生じた場合、出力先は実行時のカレントディレクトリになります。



(2) 出力形式の選択

解析結果レポートの出力形式をプルダウンで選択します。

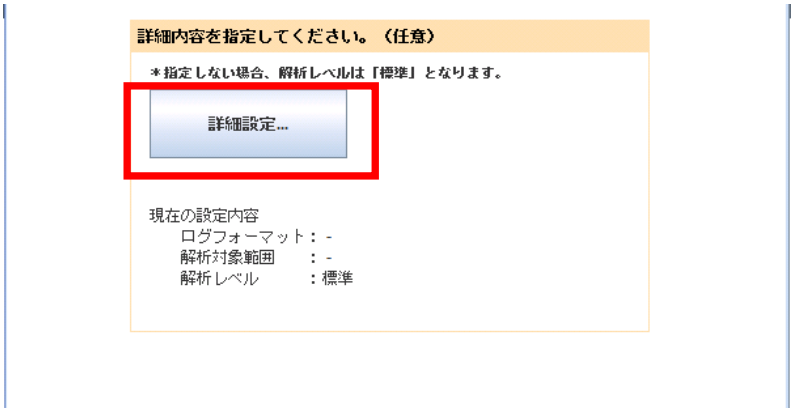


選択可能な形式は以下の通りです。「すべての形式」を選択した場合、3 つのファイルが作成されます。

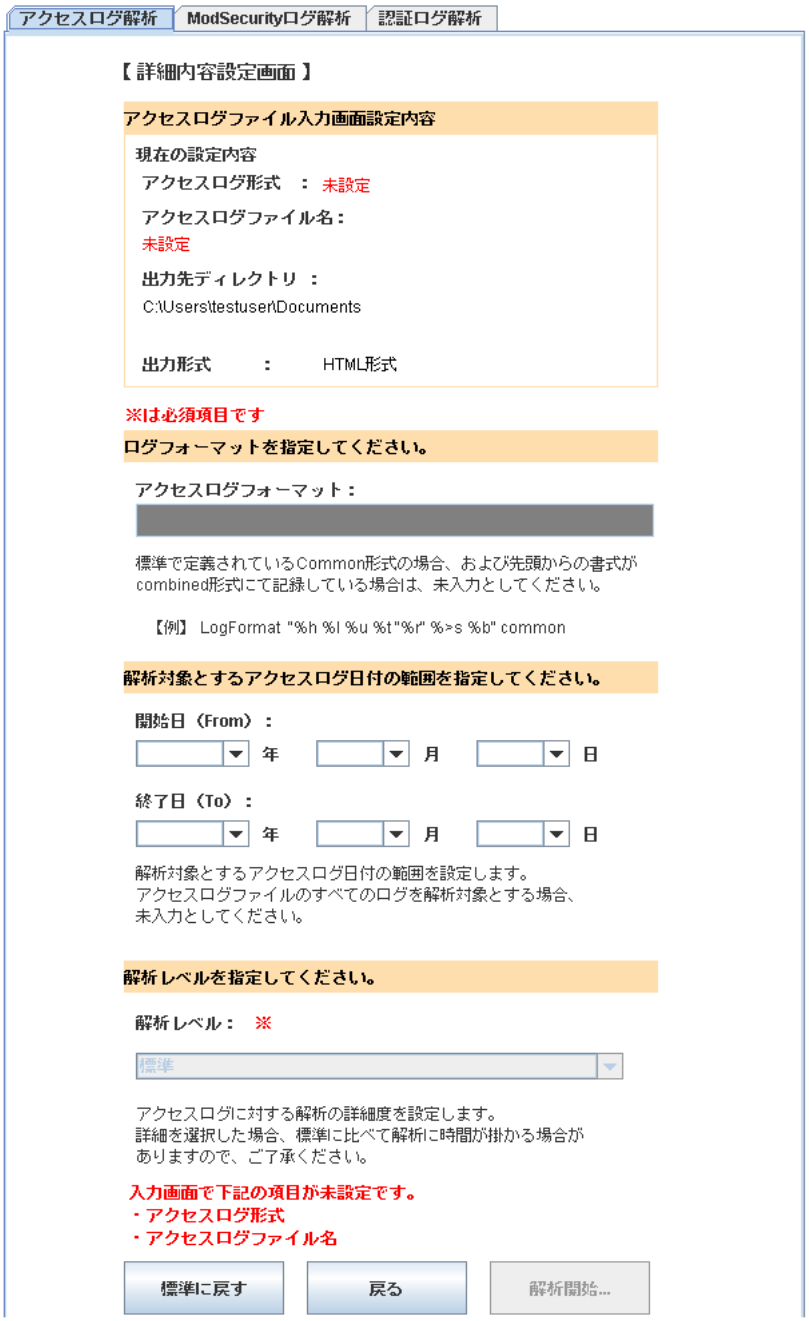
- HTML 形式
- TEXT 形式
- XML 形式
- すべての形式（HTML、XML、TEXT）

3.1.4. 詳細設定

詳細設定では、アクセスログフォーマットの指定、解析対象とする日付の範囲、解析レベルを設定できます。

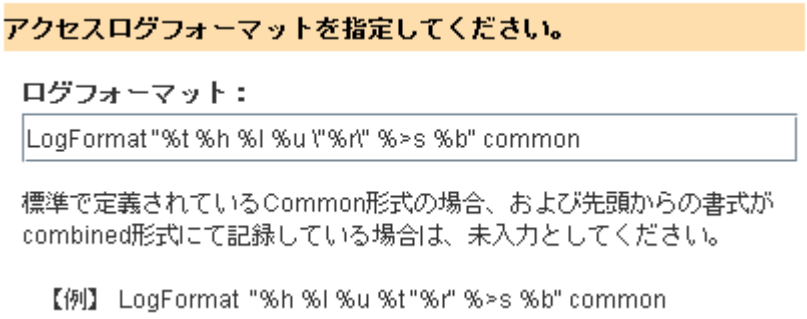


「詳細設定」ボタンを押した場合、詳細内容設定画面が表示されます。



（1） アクセスログファイルフォーマット設定

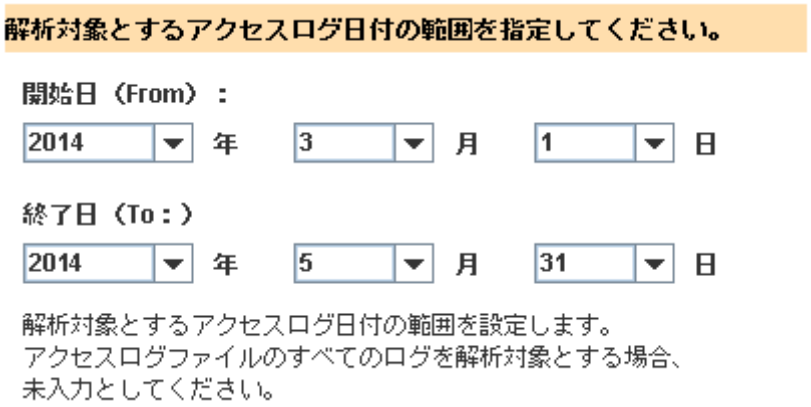
Apache1.3 系/2.0 系/2.2 系/2.4 系の common タイプのみフォーマットを指定できます。



Apache1.3 系/2.0 系/2.2 系/2. 4 系にて定義されたフォーマット文字列は 2.5.1(3)に記載されている CLF 書式の項目を参照してください。解析対象として指定されたアクセスログファイルが、設定ログフォーマットと異なる場合、エラーとして処理を行います。

（２） 日付範囲選択

解析対象のアクセスログファイルの日付範囲を指定します。



開始日のみ指定した場合、その日からのアクセスログを検出対象とします。
終了日のみ指定した場合、その日までのアクセスログを検出対象とします。
日付を指定しない場合、すべてのアクセスログを検出対象とします。

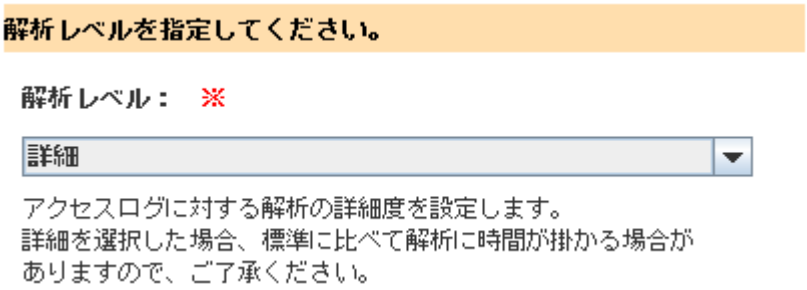
（３） 解析レベル選択

解析対象のアクセスログファイルの解析レベル「標準」「詳細」を選択します。標準レベルの検出対象脆弱性は、以下のとおりです。

- SQL インジェクション
- OS コマンド・インジェクション
- ディレクトリ・トラバーサル
- クロスサイト・スクリプティング
- その他

詳細レベルの検出対象脆弱性は、標準レベルの検出対象脆弱性と、下記の脆弱性が検出されます。

- 同一 IP アドレスからの攻撃の可能性
- アクセスログに残らない SQL インジェクション兆候
- Web サーバの設定不備を狙った攻撃の可能性



（4） 設定解除と画面遷移

「標準に戻す」ボタンを押すと、初期表示の状態に戻します。初期値について、下記のとおりです。

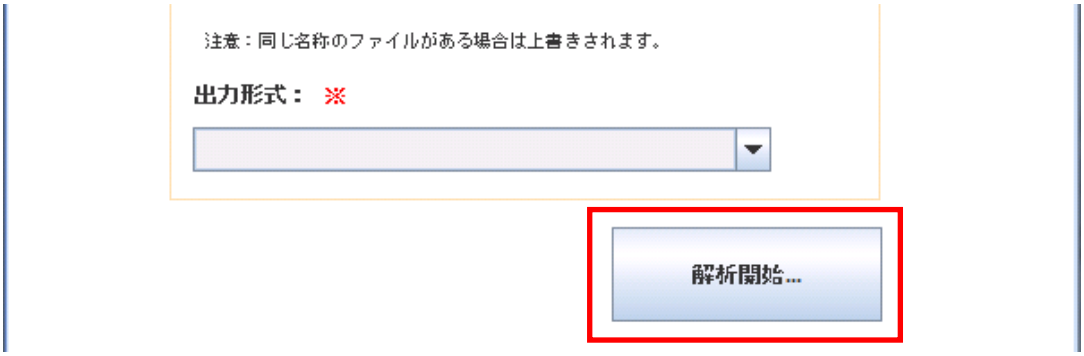
ログフォーマット：空白
開始日：空白
終了日：空白
解析レベル：標準

「戻る」ボタンを押すと、アクセスログ入力画面へ遷移します。

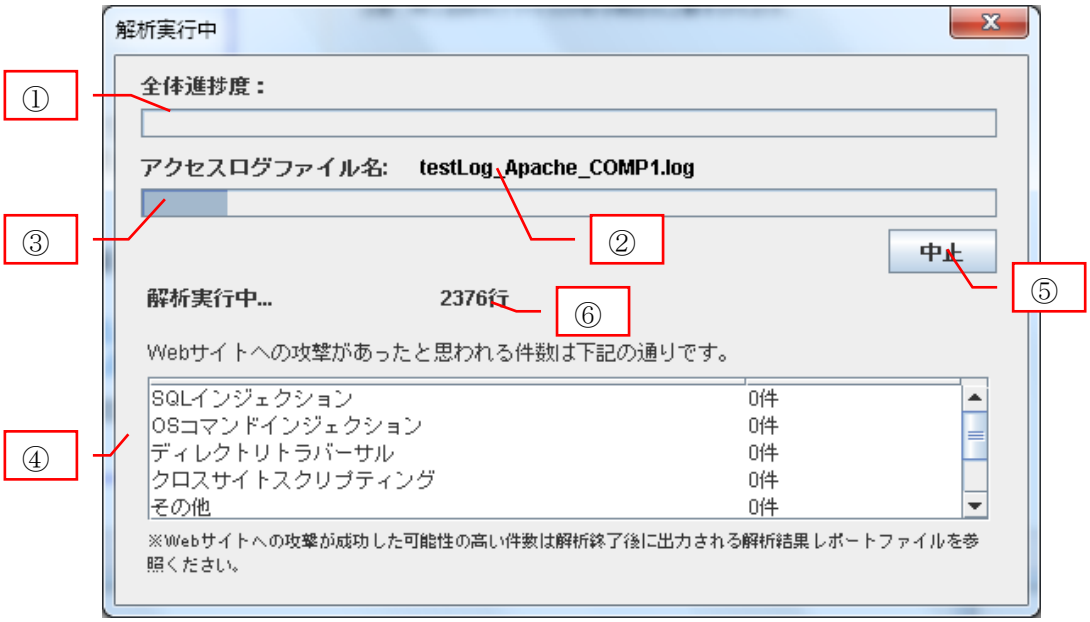
「解析開始」ボタンを押すと、設定の妥当性をチェックし、アクセスログ解析が開始されます。正しく設定されていない場合、エラーメッセージを表示し、その後解析は行われません。

3.1.5.　解析開始

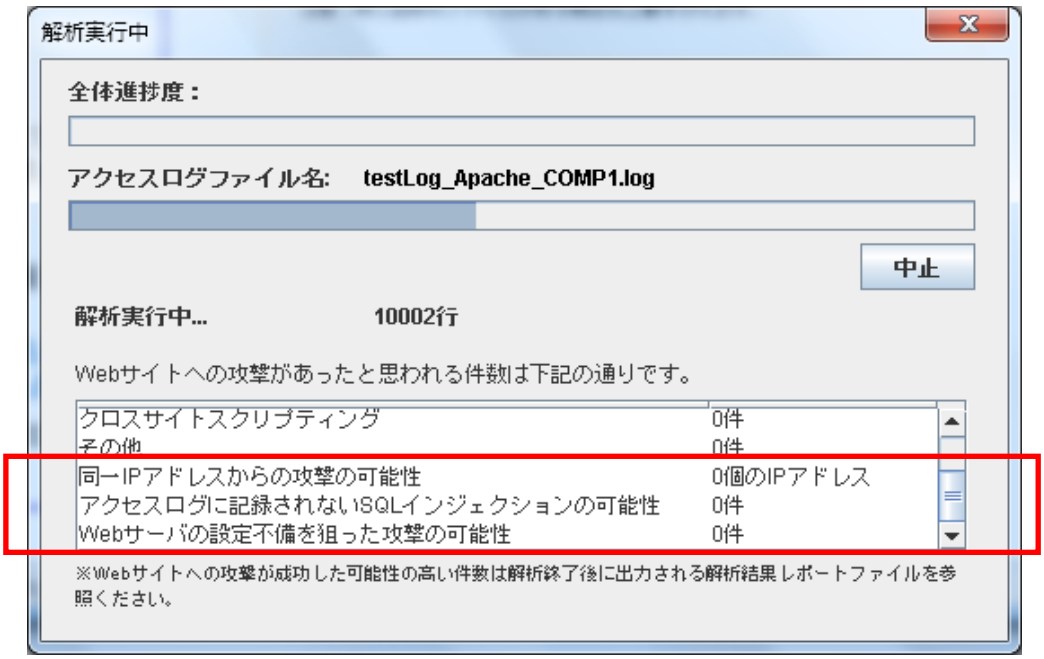
アクセスログファイル形式、解析対象アクセスログファイル、出力先ディレクトリ、出力形式をそれぞれ設定後、解析開始ボタンを押すとアクセスログ解析が開始されます。アクセスログファイル形式、解析対象アクセスログファイル、出力先ディレクトリ、出力形式が全て設定されていない場合、解析は行われません。



アクセスログ解析が開始されると、解析中画面が表示されます。解析中画面では、アクセスログ解析の進捗情報を表示します。①は全体の解析進捗状況が表示されます。②は解析中のファイル名が表示されます。③はファイル単位の解析進捗状況が表示されます。④は、検出対象脆弱性検出数がリアルタイムで表示されます。⑤は解析中止ボタンです。解析を途中で中止したい場合、このボタンを押してください。⑥は解析対象ファイルの解析した行数が表示されます。



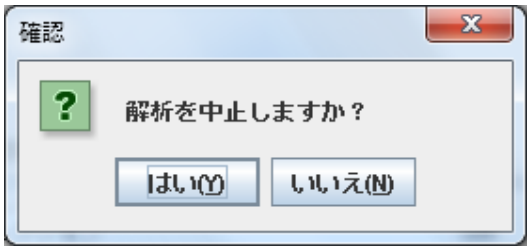
解析レベルにて「詳細」を選択した場合、以下のような解析中画面が表示されます。



中止ボタンを押した場合、確認ダイアログが表示されます。

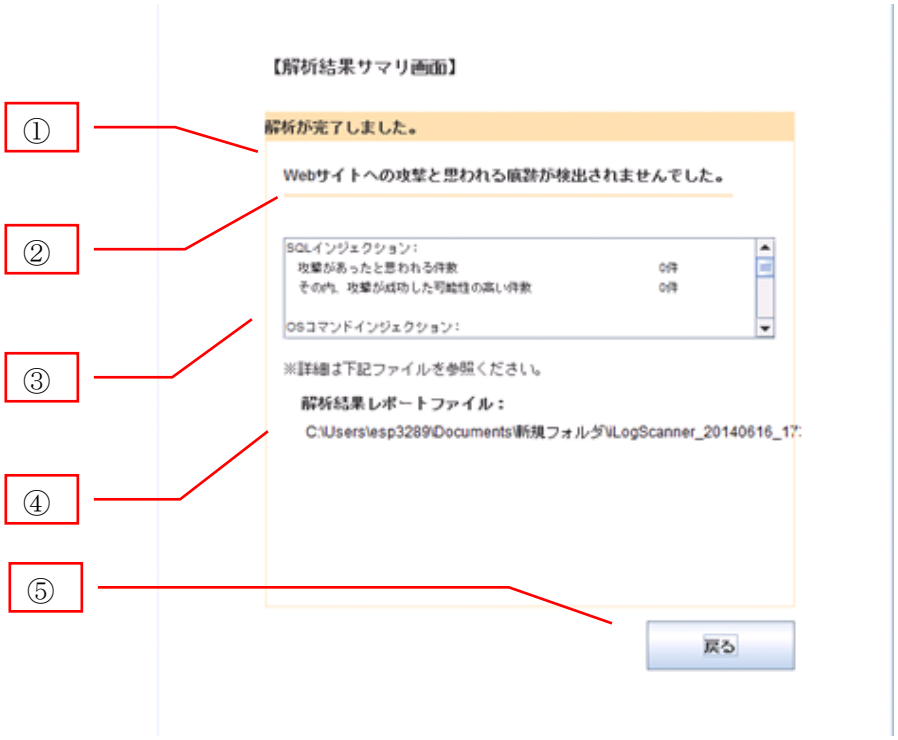
確認ダイアログの「はい」を選択した場合、処理を中止しその時点での解析結果が出力されます。

「いいえ」を選択した場合、解析実行中画面に戻ります。



3.1.6. 解析終了

アクセスログ解析が終了した後、解析結果レポートファイルを作成し、結果画面が表示されます。

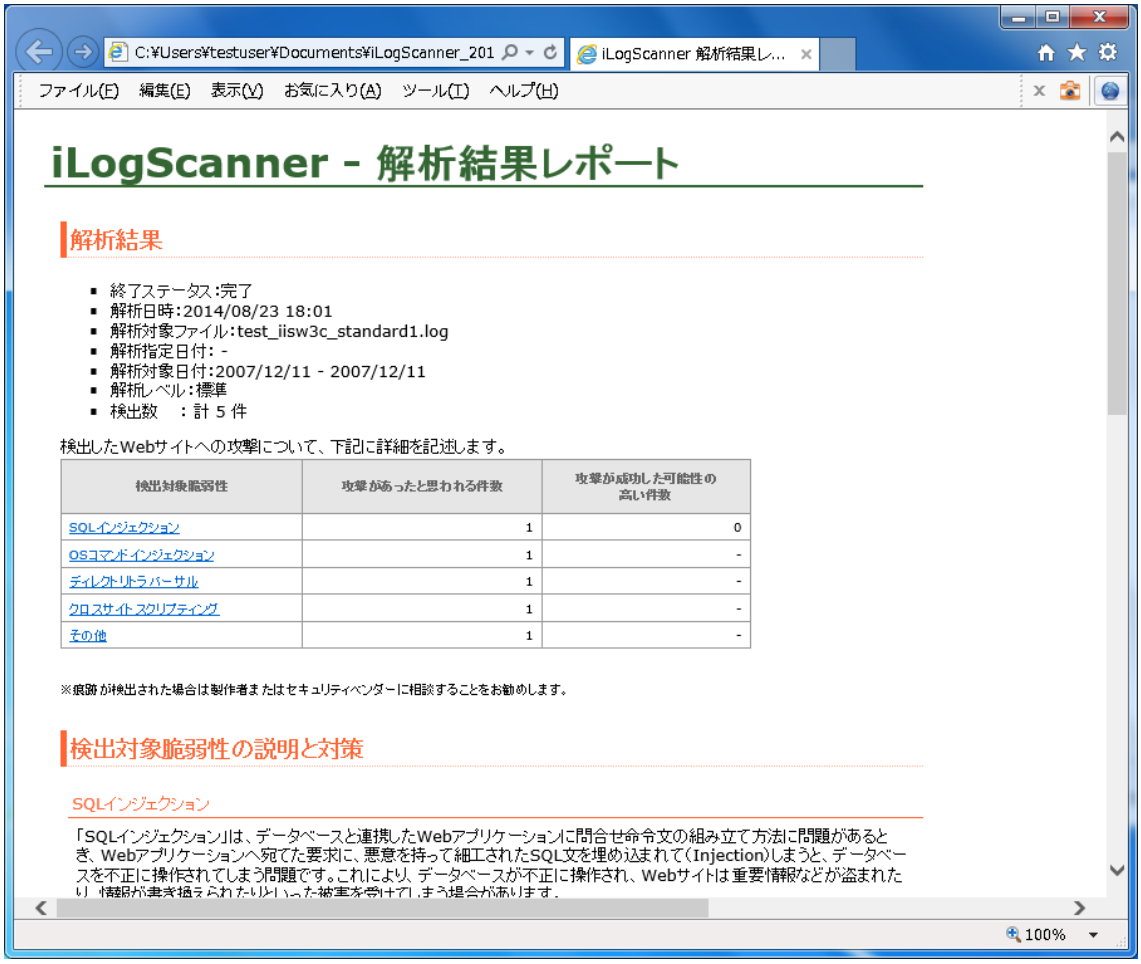


解析結果サマリ画面の①は終了メッセージ(完了/中止)が表示されます。②は攻撃痕跡の有無を示すメッセージが表示されます。③は検出対象脆弱性名と検出数が表示されます。④は解析結果レポートファイルのパス付ファイル名が表示されます。解析結果レポートファイルは、解析実行時に指定したディレクトリに出力されます。⑤の「戻る」ボタンをクリックするとアクセスログ解析画面に戻ります。

アクセスログ解析を中止した場合やエラーにより解析中止となった場合は、その時点までの解析結果を出力します。

3.1.7. 解析結果レポート

解析結果レポートは、アクセスログ解析終了後、解析前に指定した出力先ディレクトリに出力されます。HTML 形式で出力した場合の例を以下に示します。



解析結果レポートには、以下の項目が出力されます。

・解析結果

終了ステータス(完了/中止)、解析日時、解析対象ファイル、解析指定日付、解析対象日付、解析レベル、検出数が表示されます。

・検出対象脆弱性の説明と対策

iLogScanner が検出対象としている脆弱性についての説明が表示されます。対策の詳細については、下記サイトを参照ください。

-IPA　セキュリティセンターの「安全なウェブサイトの作り方」

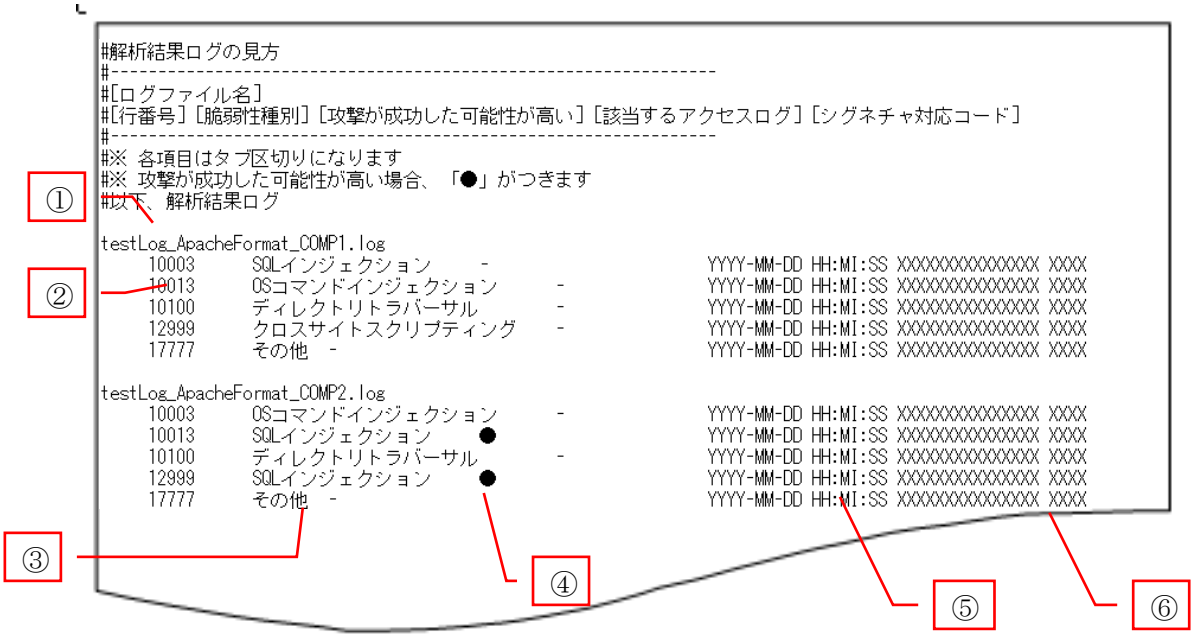
http://www.ipa.go.jp/security/vuln/websecurity.html

-IPA　セキュリティセンターの「セキュア・プログラミング講座」

http://www.ipa.go.jp/security/awareness/vendor/programmingv2/

・解析結果ログ

攻撃の痕跡を検出したログの内容を出力します。解析結果ログファイルの形式は以下のとおりです。



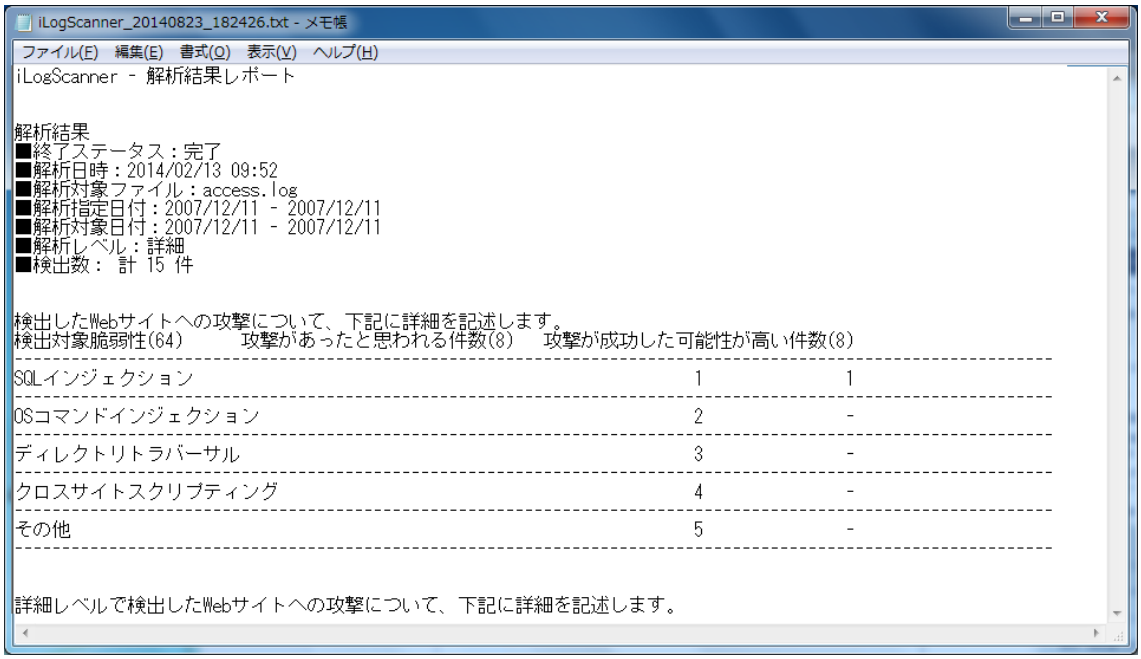

```
#解析結果ログの見方
#-----------------------------------------------------------------
#[ログファイル名]
#[行番号]［脆弱性種別］［攻撃が成功した可能性が高い］［該当するアクセスログ］［シグネチャ対応コード］
#-----------------------------------------------------------------
#※ 各項目はタブ区切りになります
#※ 攻撃が成功した可能性が高い場合、「●」がつきます
#以下、解析結果ログ

testLog_ApacheFormat_COMP1.log
     10003      SQLインジェクション      -                YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXX XXXX
     10013      OSコマンドインジェクション      -          YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXX XXXX
     10100      ディレクトリトラバーサル        -          YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXX XXXX
     12999      クロスサイトスクリプティング    -          YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXX XXXX
     17777      その他  -                                  YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXX XXXX

testLog_ApacheFormat_COMP2.log
     10003      OSコマンドインジェクション      -          YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXX XXXX
     10013      SQLインジェクション      ●                YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXX XXXX
     10100      ディレクトリトラバーサル        -          YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXX XXXX
     12999      SQLインジェクション      ●                YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXX XXXX
     17777      その他  -                                  YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXX XXXX
```

①は攻撃痕跡を検出したファイル名が出力されます。②は検出したアクセスログの行番号が出力されます。③は検出した脆弱性項目名が出力されます。④は攻撃された可能性が高い場合に「●」が出力されます。⑤は検出されたアクセスログが出力されます。⑥には内部で使用するコードが出力されます。

TEXT 形式で出力した場合の例を以下に示します。出力される項目は HTML 形式と同一です。


iLogScanner_20140823_182426.txt - メモ帳

ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

```
iLogScanner - 解析結果レポート


解析結果
■終了ステータス：完了
■解析日時：2014/02/13 09:52
■解析対象ファイル：access.log
■解析指定日付：2007/12/11 - 2007/12/11
■解析対象日付：2007/12/11 - 2007/12/11
■解析レベル：詳細
■検出数： 計 15 件


検出したWebサイトへの攻撃について、下記に詳細を記述します。
検出対象脆弱性(64)        攻撃があったと思われる件数(8)    攻撃が成功した可能性が高い件数(8)
-------------------------------------------------------------------------------
SQLインジェクション                                    1               1
-------------------------------------------------------------------------------
OSコマンドインジェクション                             2               -
-------------------------------------------------------------------------------
ディレクトリトラバーサル                               3               -
-------------------------------------------------------------------------------
クロスサイトスクリプティング                           4               -
-------------------------------------------------------------------------------
その他                                                 5               -
-------------------------------------------------------------------------------


詳細レベルで検出したWebサイトへの攻撃について、下記に詳細を記述します。
```

XML 形式のレポートについては付録を参照してください。

3.2. ModSecurity ログ解析機能の操作方法

ModSecurity ログ解析機能では、Apache アクセスログファイルおよび ModSecurity のエラーログファイルの解析を行い、解析結果を出力します。

アクセスログ／エラーログ解析のために必要な項目を入力し、解析を実行すると、解析実行中画面が表示され、進捗状況を確認することができます。アクセスログ／エラーログ解析後は、解析結果レポートを作成し、結果画面が表示されます。

アクセスログファイルのみを指定した場合に、基本の解析を行い、解析結果を出力します。

アクセスログとエラーログ両方とも指定した場合、アクセスログの基本の解析後、アクセスログの解析結果とエラーログのマッチング機能を実行します。

Apache HTTP Server エラーログファイルのみを指定した場合、ModSecurity で検出・遮断したデータを解析し、統計情報を出力します。

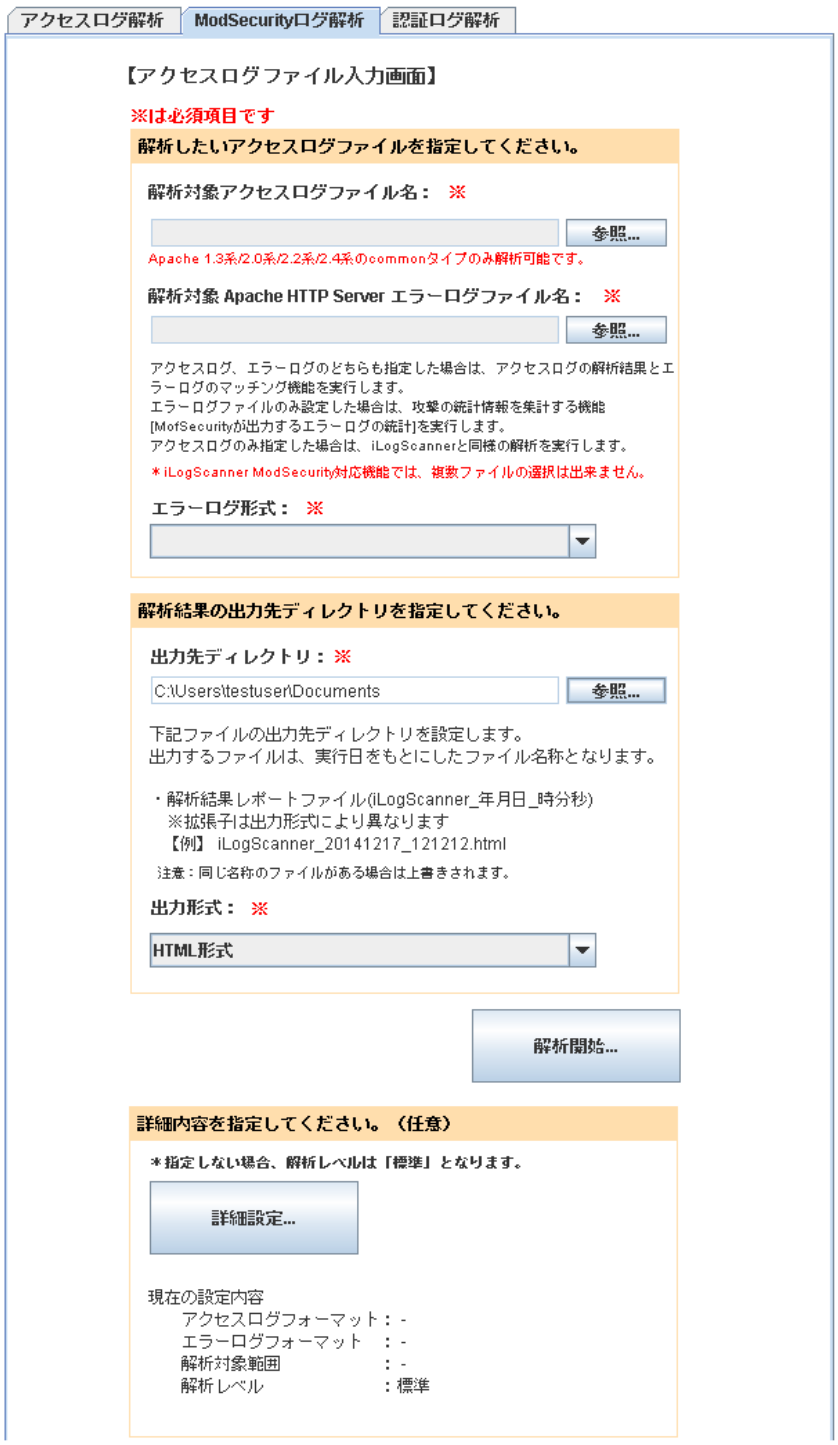
※ アクセスログ形式は、Apache1.3 系/2.0 系/2.2 系/2.4 系の common タイプのみ対応しております

※ 解析対象ファイルを複数選択することはできません

3.2.1. 初期画面表示

iLogScanner トップページで、オンライン版 iLogScanner の利用許諾内容を確認し、利用許諾に同意される方は「利用許諾に同意する」をチェックして「オンライン版 iLog Scanner を起動する」ボタンを押して下さい。iLogScanner が起動し、初期画面が表示されたら、「ModSecurity ログ解析」のタブを選択してください。

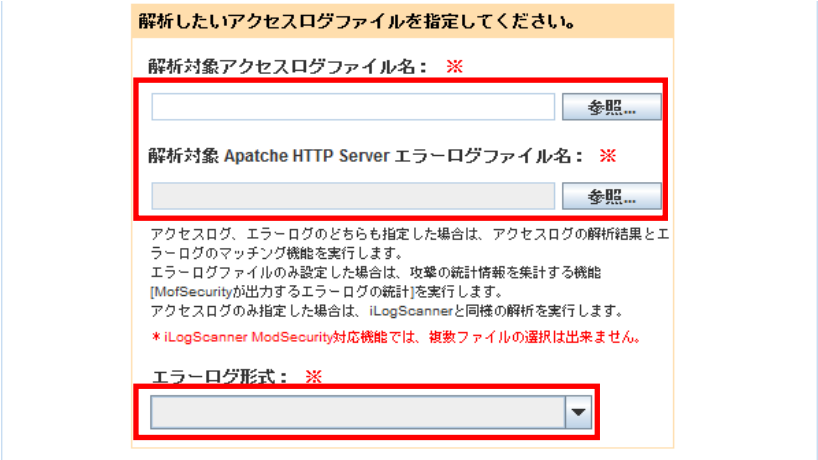
「利用許諾に同意する」をチェックしていない場合、iLogScanner は起動しません。



3.2.2. 解析対象ファイルの指定

解析を行うアクセスログファイルあるいはエラーログファイルを指定します。

「参照」ボタンを押すと、ファイル選択画面が表示されます。エラーログ形式はプルダウンで選択します。



選択可能なエラーログ形式は以下の通りです。

・Apache1.3 系/2.0 系/2.2 系のエラーログタイプ

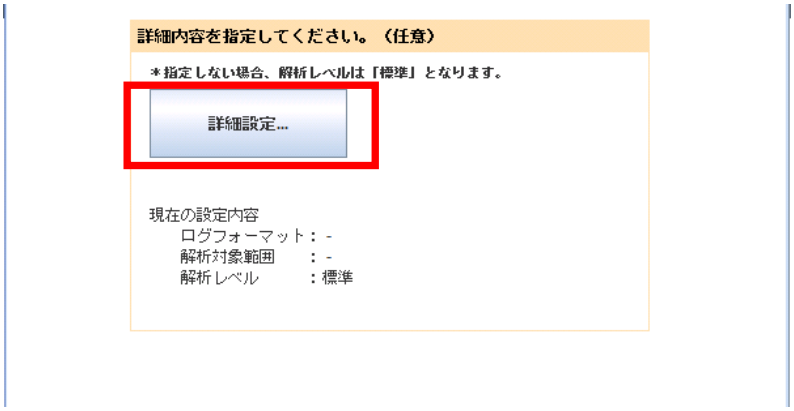
・Apache2.4 系のエラーログタイプ

3.2.3. 解析結果出力の設定

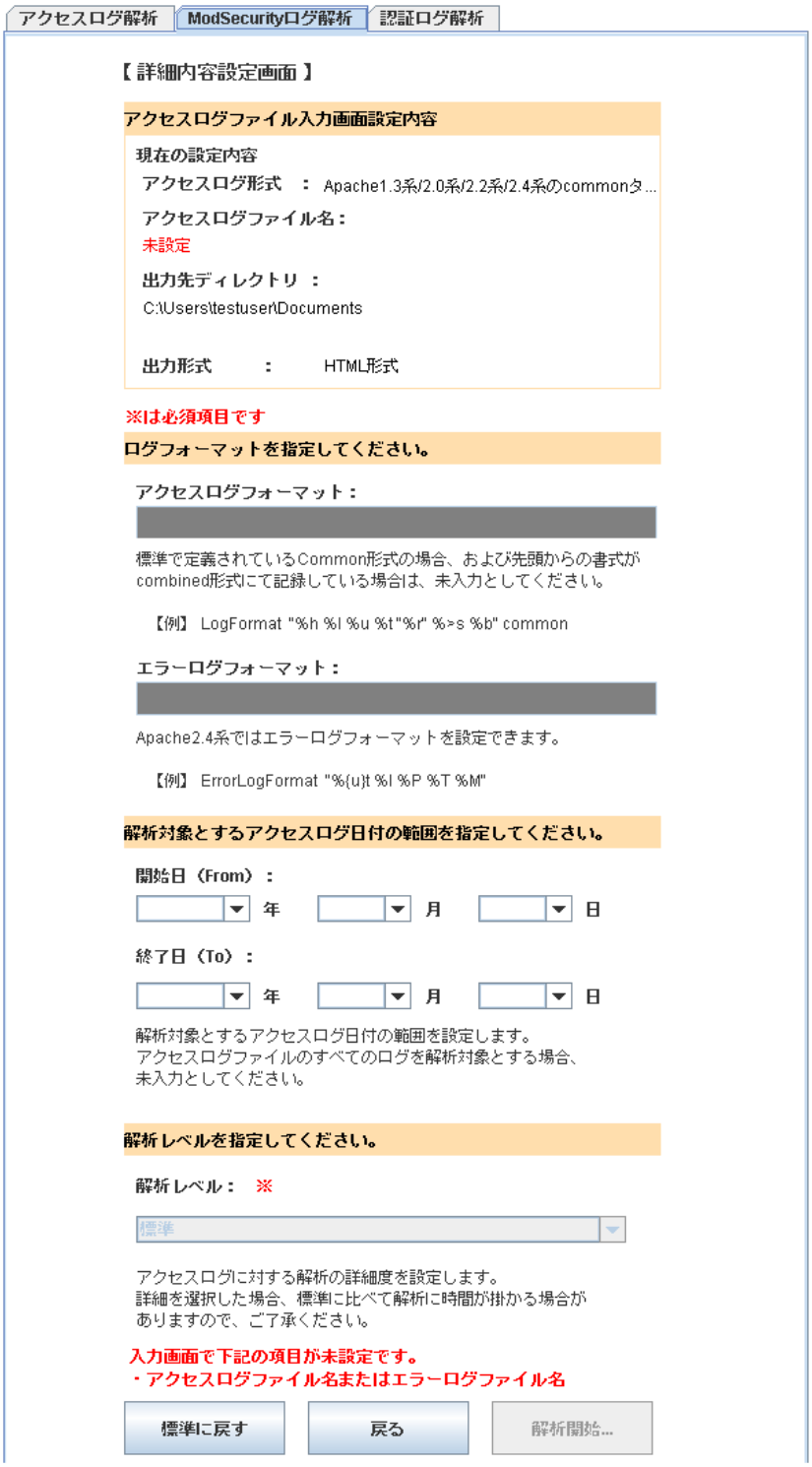
「3.1.3 解析結果出力の設定」を参照してください。

3.2.4. 詳細設定

詳細設定では、アクセスログ／エラーログフォーマットの指定、解析対象とする日付の範囲、解析レベルを設定できます。

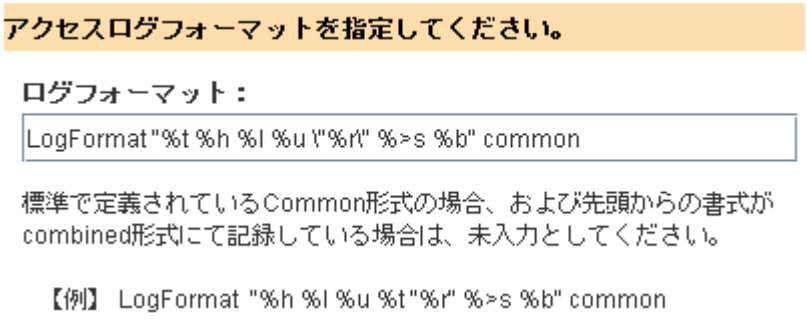


「詳細設定」ボタンを押した場合、詳細内容設定画面が表示されます。


アクセスログ解析
ModSecurityログ解析
認証ログ解析
【詳細内容設定画面】
アクセスログファイル入力画面設定内容
現在の設定内容
アクセスログ形式 ： Apache1.3系/2.0系/2.2系/2.4系のcommonタ...
アクセスログファイル名：
未設定
出力先ディレクトリ ：
C:\Users\testuser\Documents
出力形式 ： HTML形式
※は必須項目です
ログフォーマットを指定してください。
アクセスログフォーマット：
標準で定義されているCommon形式の場合、および先頭からの書式がcombined形式にて記録している場合は、未入力としてください。
【例】 LogFormat "%h %l %u %t "%r" %>s %b" common
エラーログフォーマット：
Apache2.4系ではエラーログフォーマットを設定できます。
【例】 ErrorLogFormat "%{u}t %l %P %T %M"
解析対象とするアクセスログ日付の範囲を指定してください。
開始日（From）：
年 月 日
終了日（To）：
年 月 日
解析対象とするアクセスログ日付の範囲を設定します。
アクセスログファイルのすべてのログを解析対象とする場合、
未入力としてください。
解析レベルを指定してください。
解析レベル： ※
標準
アクセスログに対する解析の詳細度を設定します。
詳細を選択した場合、標準に比べて解析に時間が掛かる場合があ
りますので、ご了承ください。
入力画面で下記の項目が未設定です。
・アクセスログファイル名またはエラーログファイル名
標準に戻す
戻る
解析開始...

（1） アクセスログファイルフォーマット設定

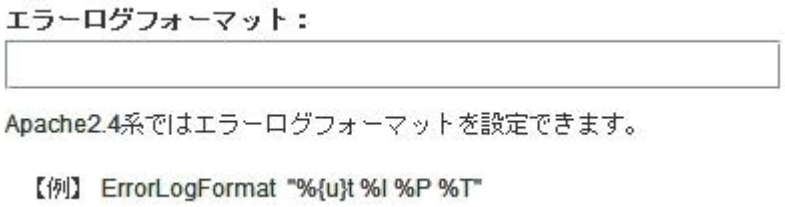
Apache1.3 系/2.0 系/2.2 系/2.4 系の common タイプのみフォーマットを指定できます。



Apache1.3 系/2.0 系/2.2 系/2. 4 系にて定義されたフォーマット文字列は 2.5.1(3)に記載されている CLF 書式の項目を参照してください。解析対象として指定されたアクセスログファイルが、設定ログフォーマットと異なる場合、エラーとして処理を行います。

（2） エラーログフォーマット

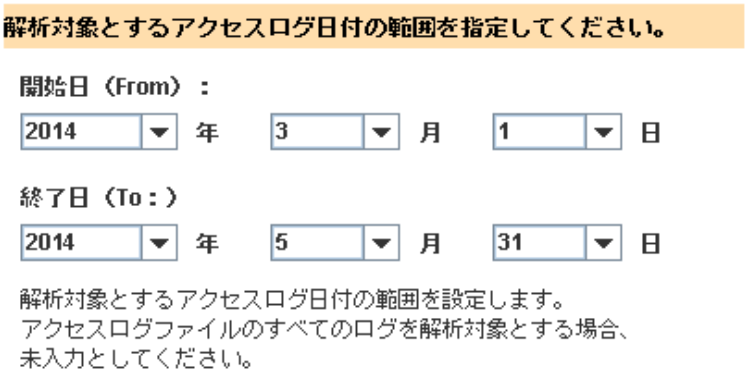
Apache2.4 系のエラーログタイプを選択した場合、エラーログフォーマットを指定できます。



指定可能なフォーマット文字列は 2.5.2(2)を参照してください。解析対象として指定されたアクセスログファイルが、設定ログフォーマットと異なる場合、エラーとして処理を行います。

（３） 日付範囲選択

解析対象のアクセスログファイルの日付範囲を指定します。



開始日のみ指定した場合、その日からのアクセスログを検出対象とします。
終了日のみ指定した場合、その日までのアクセスログを検出対象とします。
日付を指定しない場合、すべてのアクセスログを検出対象とします。

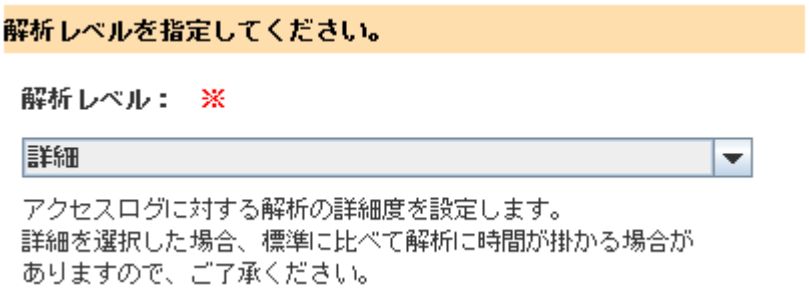
（４） 解析レベル選択

解析対象のアクセスログファイルの解析レベル「標準」「詳細」を選択します。標準レベルの検出対象脆弱性は、以下のとおりです。

- SQL インジェクション
- OS コマンド・インジェクション
- ディレクトリ・トラバーサル
- クロスサイト・スクリプティング
- その他

詳細レベルの検出対象脆弱性は、標準レベルの検出対象脆弱性と、下記の脆弱性が検出されます。

- 同一 IP アドレスからの攻撃の可能性
- アクセスログに残らない SQL インジェクション兆候
- Web サーバの設定不備を狙った攻撃の可能性



（５） 設定解除と画面遷移

「標準に戻す」ボタンを押すと、初期表示の状態に戻します。初期値について、下記のとおりです。

ログフォーマット：空白

開始日：空白

終了日：空白

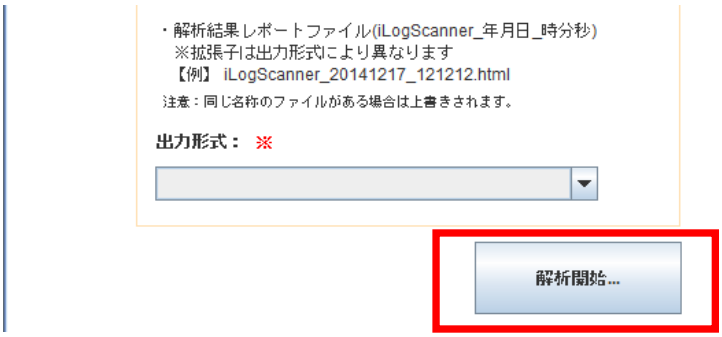
解析レベル：標準

「戻る」ボタンを押すと、アクセスログ／エラーログ入力画面へ遷移します。

「解析開始」ボタンを押すと、設定の妥当性をチェックし、アクセスログ／エラーログ解析が開始されます。正しく設定されていない場合、エラーメッセージを表示し、その後解析は行われません。

3.2.5.　解析開始

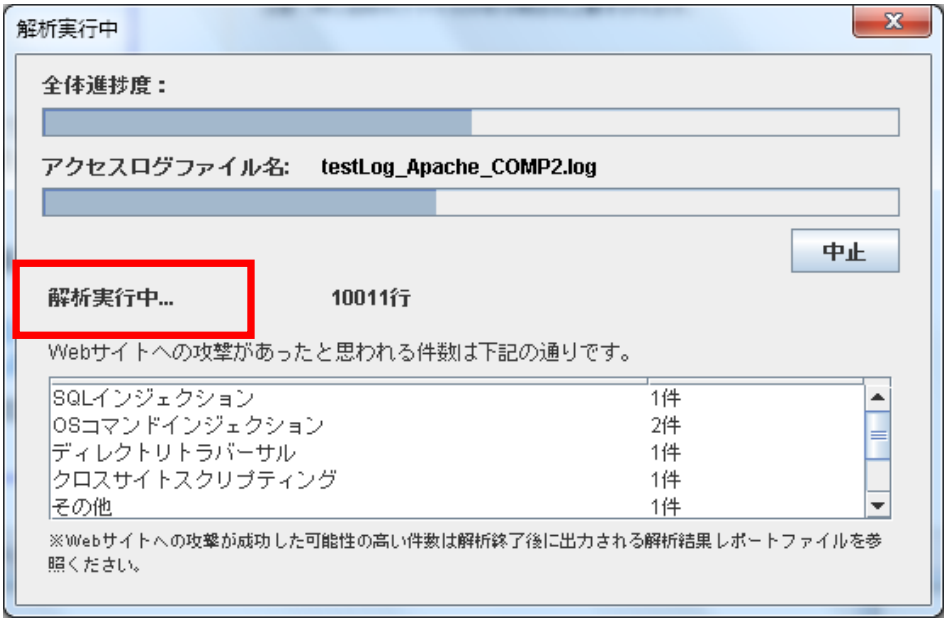
解析対象アクセスログファイル／エラーログファイル、出力先ディレクトリ、出力フォーマットをそれぞれ設定後、解析開始ボタンを押すと解析が開始されます。解析対象ファイル、出力先ディレクトリ、出力フォーマットが全て設定されていない場合、解析は行われません。



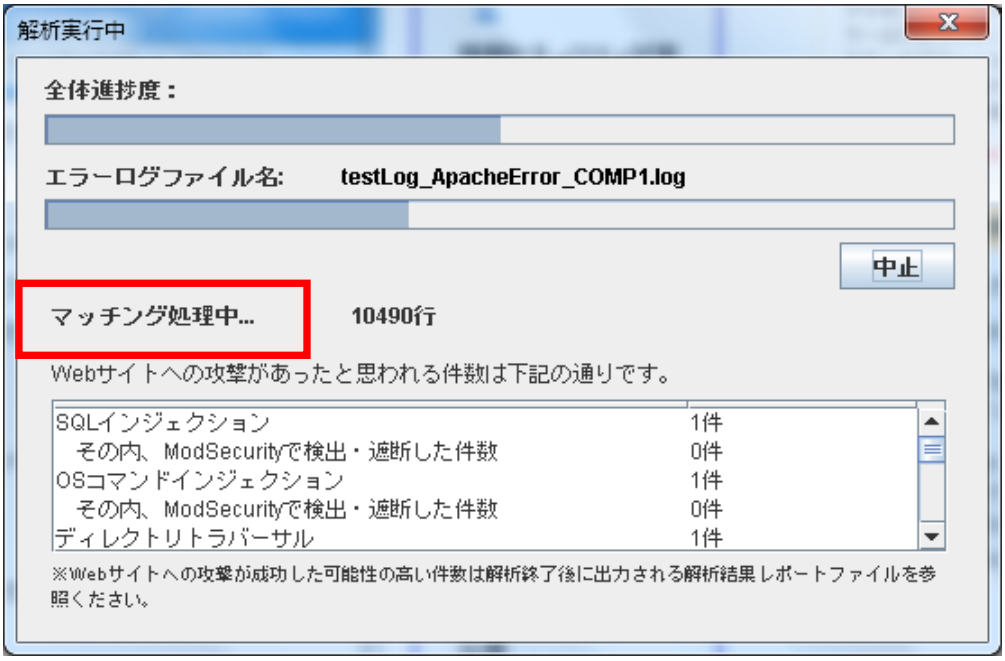
(1) アクセスログファイルのみを指定した場合、解析実行中画面は「3.1.5　解析開始」を参照してください。

(2) アクセスログとエラーログファイル両方を指定した場合、解析が開始されると、解析実行中画面は以下の通りに表示されます。

アクセスログファイル解析中

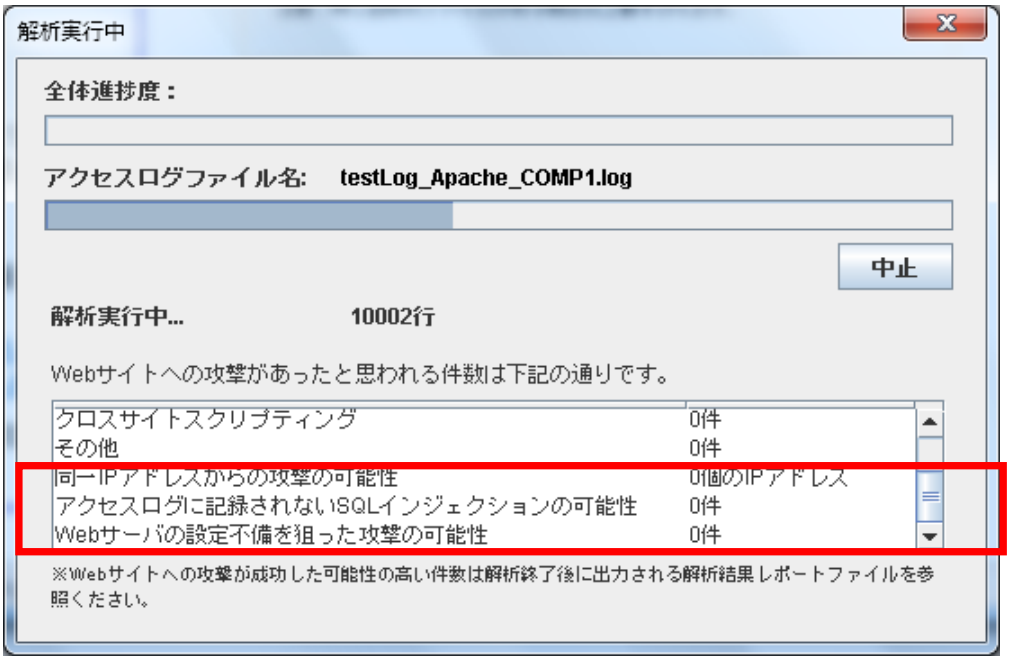


エラーログのマッチング処理中、ModSecurity で検出・遮断した件数が表示されます。

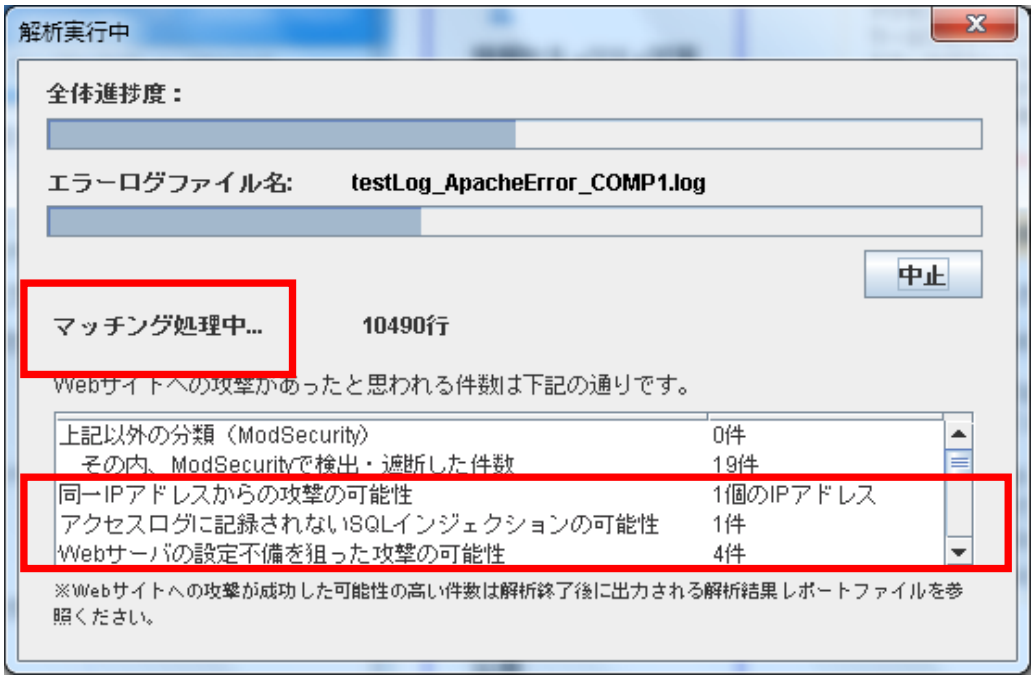


解析レベルにて「詳細」を選択した場合、以下のような画面が表示されます。

アクセスログファイル解析中

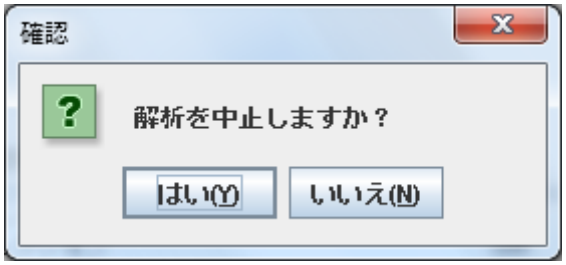


エラーログのマッチング処理中



(3) エラーログファイルのみを指定した場合の動作は、「3.2.8　ログ統計情報レポート出力機能」を参照してください。

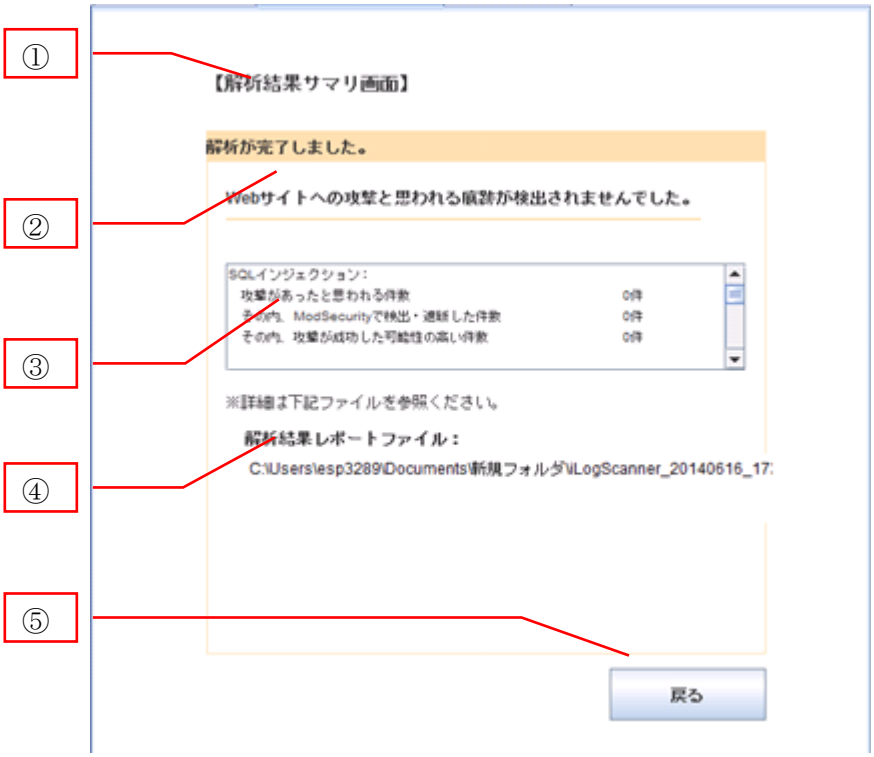
中止ボタンを押した場合、確認ダイアログが表示されます。確認ダイアログの「はい」を選択した場合、処理を中止しその時点での解析結果が出力されます。「いいえ」を選択した場合、解析実行中画面に戻ります。



3.2.6.　解析終了

アクセスログ／エラーログ解析が終了した後、解析結果レポートファイルを作成し、結果画面が表示されます。

※　解析対象エラーログファイルのみで選択した場合、統計情報レポートファイルを作成します。「3.2.8　ログ統計情報レポート出力」を参照してください。



解析結果サマリ画面の①は終了メッセージ(完了/中止)が表示されます。②は攻撃痕跡の有無を示すメッセージが表示されます。③は検出対象脆弱性名と ModSecurity で検出・遮断した件数が表示されます。④は解析結果レポートファイルのパス付ファイル名が表示されます。解析結果レポートファイルは、解析実行時に指定したディレクトリに出力されます。⑤の「戻る」ボタンをクリックすると ModSecurity ログ解析画面に戻ります。

ModSecurity ログ解析を中止した場合やエラーにより解析中止となった場合は、その時点までの解析結果を出力します。

3.2.7. 解析結果レポート

解析結果レポートは、アクセスログ解析終了後、解析前に指定した出力先ディレクトリに出力されます。HTML 形式で出力した場合の例を以下に示します。

解析結果レポートには、以下の項目が出力されます。

・解析結果

終了ステータス(完了/中止)、解析日時、解析対象ファイル、解析対象エラーログファイル、解析指定日付、解析対象日付、解析レベル、検出数（ModSecurity で検出・遮断した件数）が表示されます。解析レベルで「詳細」を指定した場合、検出したウェブサイトへの攻撃についての詳細と、注意喚起メッセージが表示されます。

・検出対象脆弱性の説明と対策

iLogScanner が検出対象としている脆弱性についての説明が表示されます。対策の詳細については、下記サイトを参照ください。

-IPA　セキュリティセンターの「安全なウェブサイトの作り方」

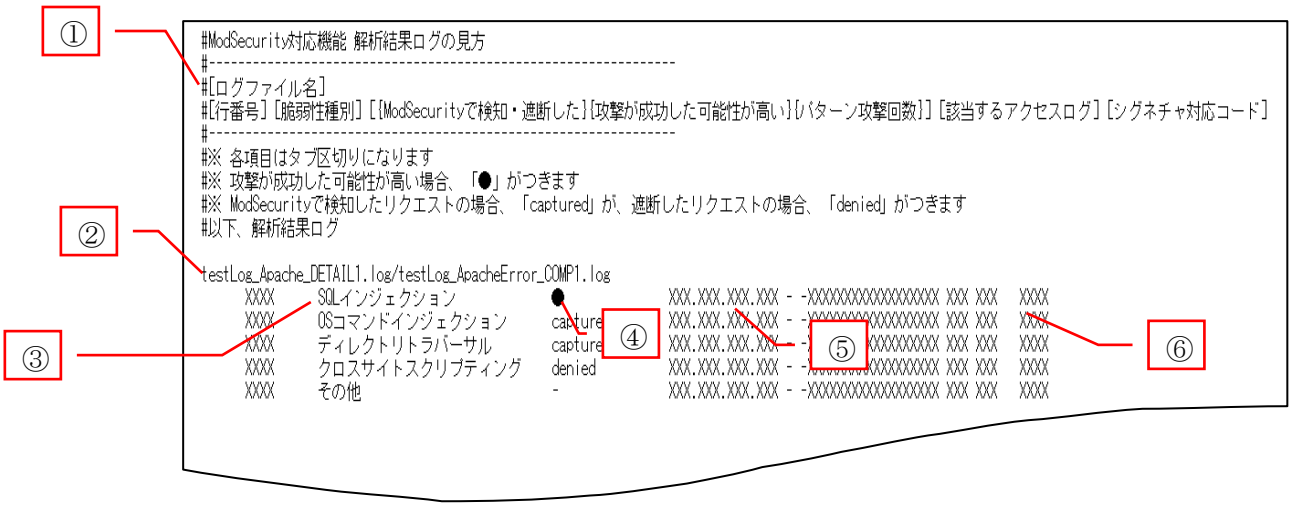
http://www.ipa.go.jp/security/vuln/websecurity.html

-IPA　セキュリティセンターの「セキュア・プログラミング講座」

http://www.ipa.go.jp/security/awareness/vendor/programmingv2/

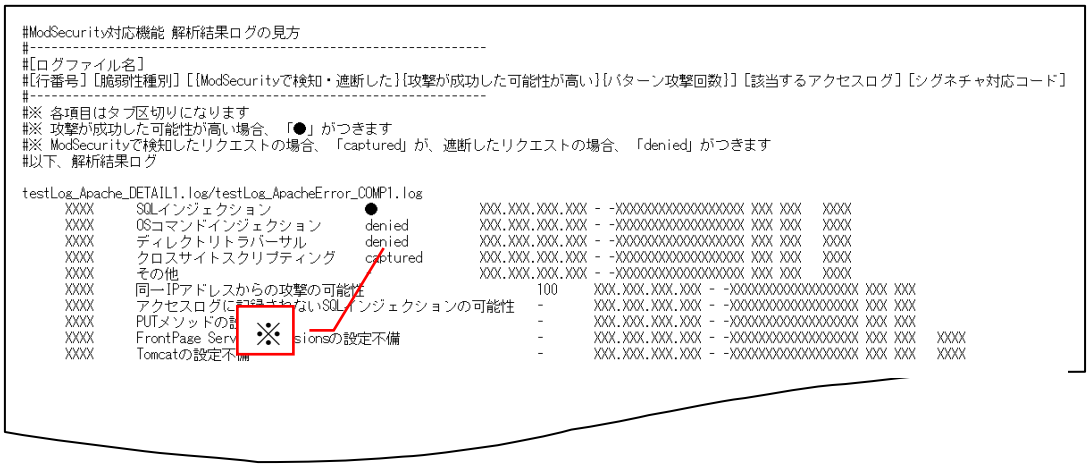
・解析結果ログ

攻撃の痕跡を検出したログの内容を出力します。解析結果ログファイルの形式は以下のとおりです。



①は攻撃痕跡を検出した解析対象ファイル名が出力されます。②は検出したアクセスログの行番号が出力されます。③は検出した脆弱性項目名が出力されます。④は攻撃された可能性が高い場合に「●」が出力されます。※⑤は検出されたアクセスログが出力されます。⑥には内部で使用するコードが出力されます。

解析レベルにて「詳細」を選択した場合に、下のような解析結果ログが出力されます。



※ModSecurity で遮断した場合、値：「denied」

ModSecurity で検出した場合、値：「captured」

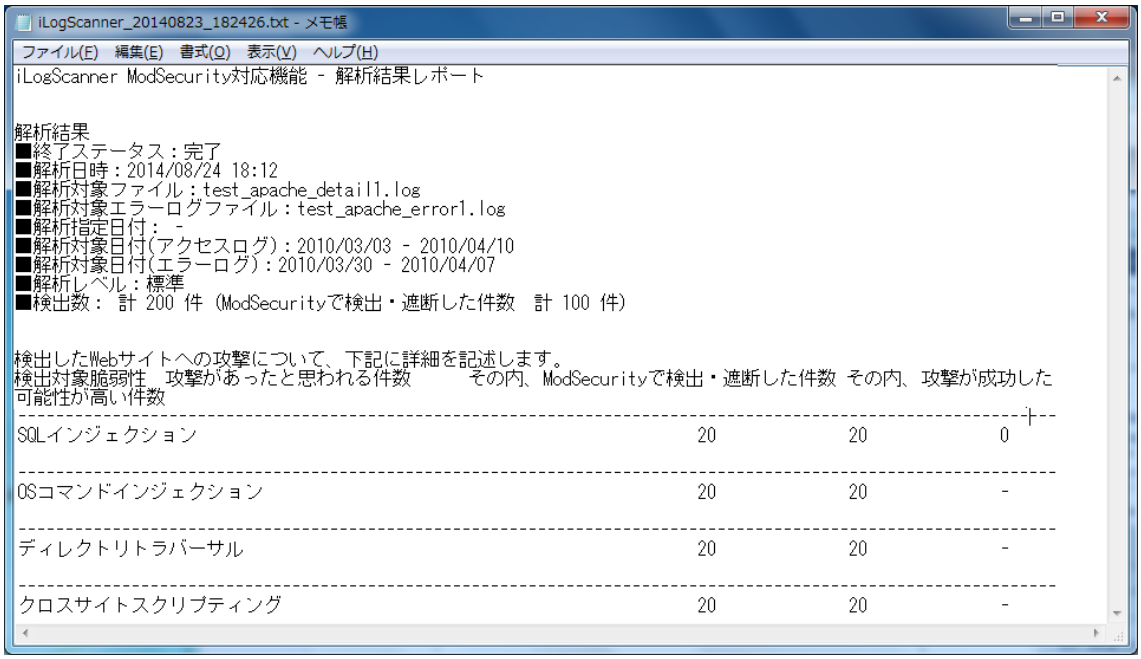
ModSecurity で遮断かどうか不明の場合、値：「deficiency」

攻撃が成功した可能性が高い場合、値：「●」

同一 IP アドレスからの攻撃を検出した場合、検出数を表示　値：「XXX」

攻撃か成功した可能性について不明の場合、値：「-」

TEXT 形式で出力した場合の例を以下に示します。出力される項目は HTML 形式と同一です。

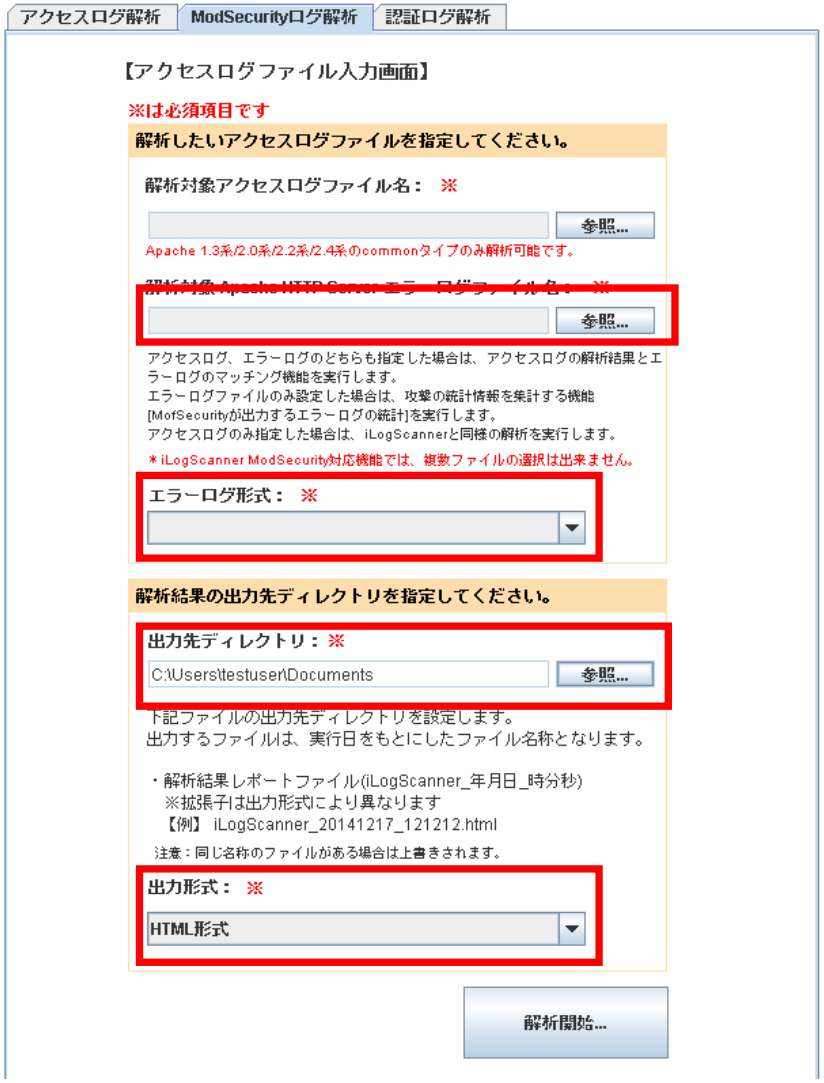


XML 形式のレポートについては付録を参照してください。

3.2.8.　ログ統計情報レポート出力機能

ModSecurity から出力されるエラーログファイルを解析し、攻撃の情報を集計する機能です。解析対象エラーログファイルのみで選択した場合、統計情報レポートファイルを作成します。

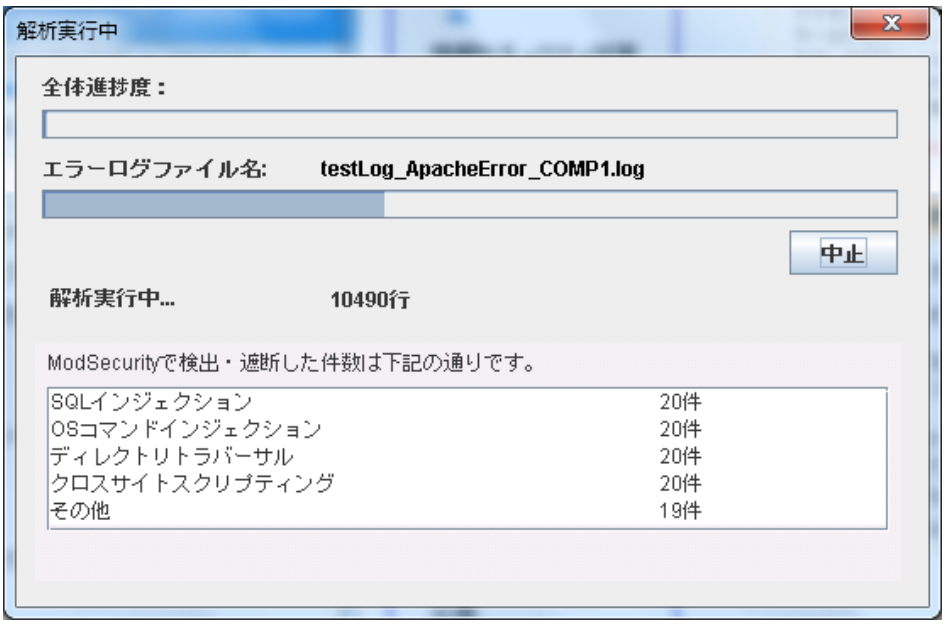
(1)　操作手順



エラーログファイルエラーログ形式、出力先ディレクトリと出力形式を選択後、解析開始ボタンを押すとエラーログ解析が開始されます。選択ファイルが指定された Apache のエラーログ形式ではない場合、解析は行われません。オプション設定画面で集計対象日付を指定することができます。

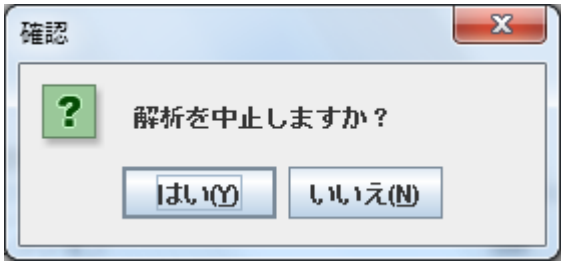
(2)　解析開始

エラーログファイル解析中、ModSecurity で検出・遮断した件数が表示されます。



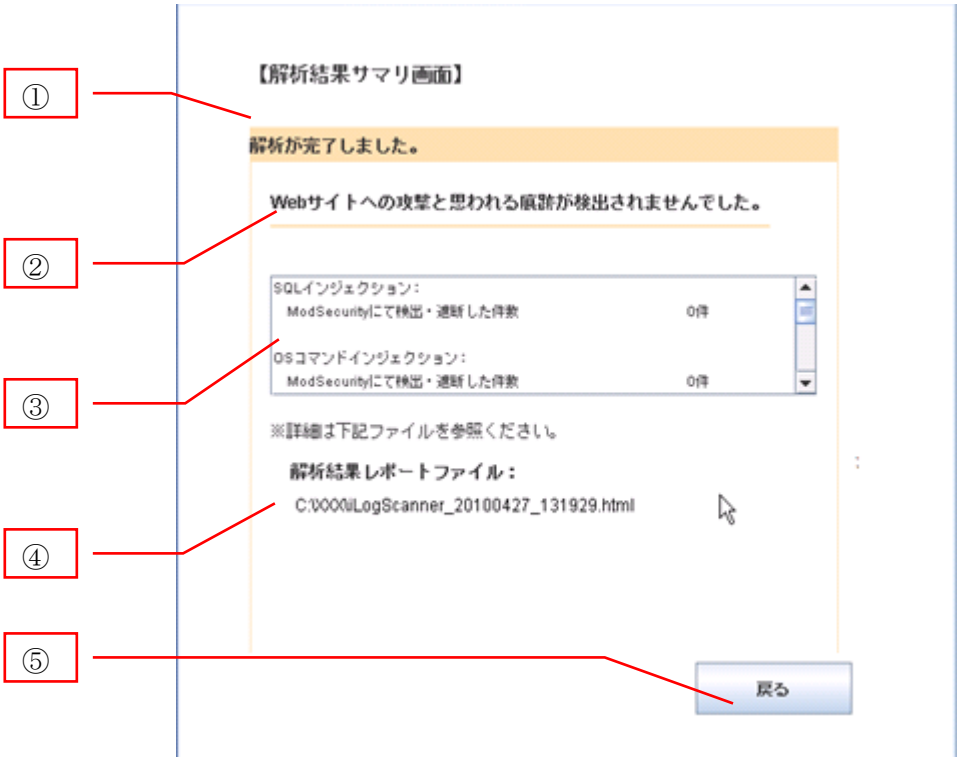
中止ボタンを押した場合、確認ダイアログが表示されます。

確認ダイアログの「はい」を選択した場合、処理を中止しその時点での統計結果が出力されます。「いいえ」を選択した場合、解析実行中画面に戻ります。



(3)　解析終了

解析が終了した後、結果画面が表示されます。



解析結果サマリ画面の①は終了メッセージ(完了/中止)が表示されます。②は攻撃痕跡の有無を示すメッセージが表示されます。③は検出対象脆弱性名と ModSecurity で検出・遮断した件数が表示されます。④は解析結果レポートファイルのパス付ファイル名が表示されます。解析結果レポートファイルは、解析実行時に指定したディレクトリに出力されます。⑤の「戻る」ボタンをクリックすると ModSecurity ログ解析画面に戻ります。

ModSecurity ログ解析を中止した場合やエラーにより解析中止となった場合は、その時点までの解析結果を出力します。

(4) 統計情報レポート

統計結果レポートは解析前に指定した出力先ディレクトリに出力されます。
HTML 形式で出力した場合の例を以下に示します。

統計情報レポートには、以下の項目が出力されます。

・解析結果

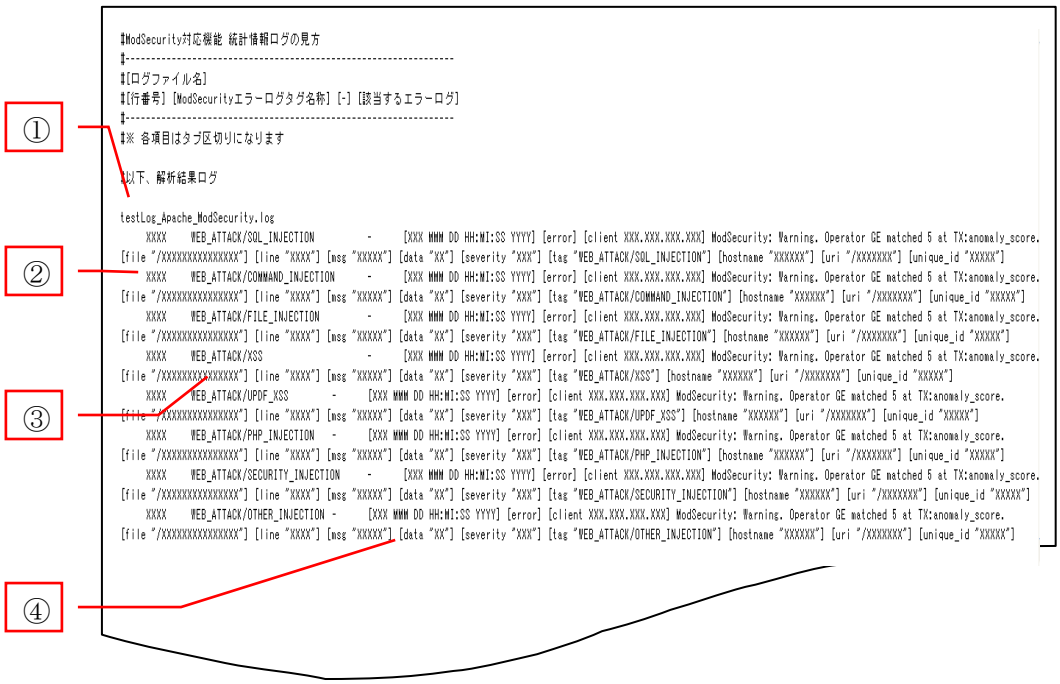
終了ステータス(完了/中止)、解析日時、解析対象エラーログファイル、解析指定日付、解析対象日付、解析レベル、検出数が表示されます。

・検出対象脆弱性の説明と対策

iLogScanner が検出対象としている脆弱性についての説明が表示されます。また、集計対象としている脆弱性の tag 名称（ModSecurity で検知した脆弱性種別を表す文字列）が表示されます。

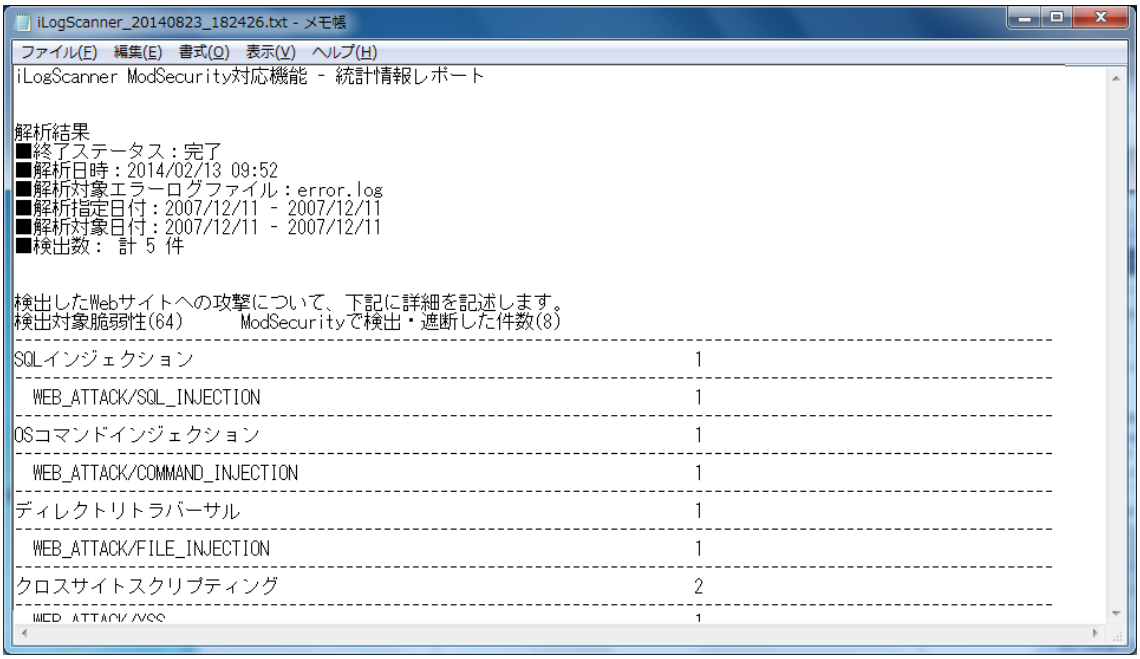
・解析結果ログ

攻撃の痕跡を検出したログの内容を出力します。解析結果ログファイルの形式は以下のとおりです。



①は攻撃痕跡を検出したエラーログファイル名が出力されます。②は検出したアクセスログの行番号が出力されます。③は検出した脆弱性の tag 名称が出力されます。④は検出されたエラーログデータが出力されます。

TEXT 形式で出力した場合の例を以下に示します。出力される項目は HTML 形式と同一です。



XML 形式のレポートについては付録を参照してください。

3.3. 認証ログ解析機能の操作方法

認証ログ解析機能では、sshd のログファイル（syslog）および vsftpd のログファイルの解析を行い、解析結果を出力します。

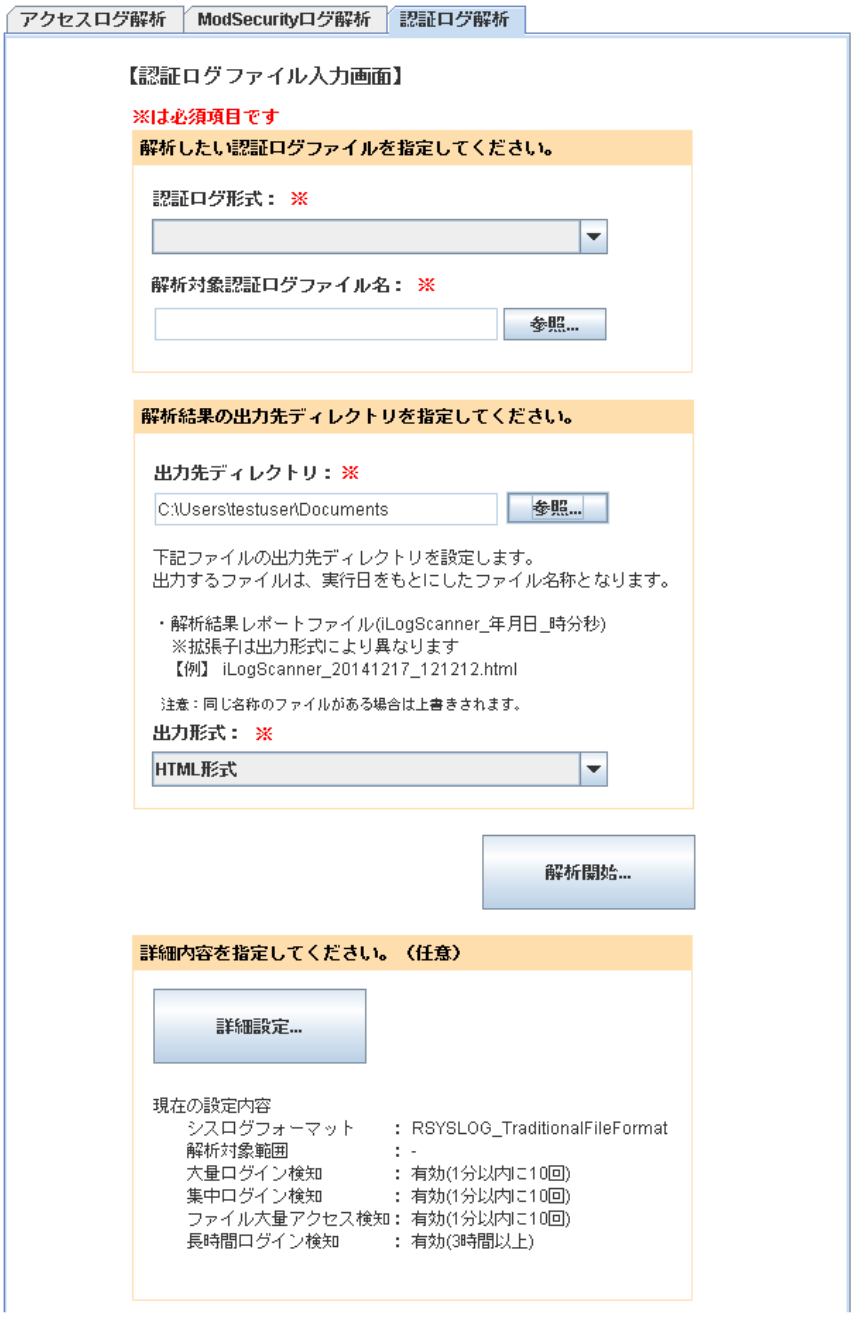
認証ログ解析のために必要な項目を入力し、解析を実行すると、解析実行中画面が表示され、進捗状況を確認することができます。認証ログ解析後は、解析結果レポートを作成し、結果画面が表示されます。

※ syslog のフォーマットは RSYSLOG_TraditionalFileFormat と RSYSLOG_FileFormat に対応しています。
※ vsftpd のログファイルは vsftpd 形式、wu-ftpd 形式に対応しています。
※ 解析対象ログの形式によって、検出可能な項目が異なります。

3.3.1. 初期画面表示

iLogScanner トップページで、オンライン版 iLogScanner の利用許諾内容を確認し、利用許諾に同意される方は「利用許諾に同意する」をチェックして「オンライン版 iLog Scanner を起動する」ボタンを押して下さい。iLogScanner が起動し、初期画面が表示されたら、「認証ログ解析」タブを選択してください。

「利用許諾に同意する」をチェックしていない場合、iLogScanner は起動しません。

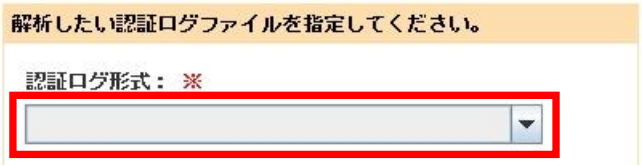


3.3.2. 解析対象ファイルの指定

解析を行うログファイルを指定します。

(1) ログ形式選択

解析を行う認証ログファイルの形式をプルダウンで指定します。

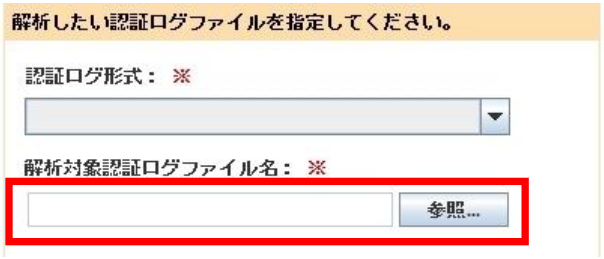


選択可能な形式は以下の通りです。

- CentOS6 系/RHEL6 系 sshd(SSH・SFTP)のログ（シスログ）
- CentOS6 系/RHEL6 系 vsftpd(FTP)の vsftpd 形式ログ
- CentOS6 系/RHEL6 系 vsftpd(FTP)の wu-ftpd 形式ログ

(2) 解析対象ログファイル指定

「参照」ボタンを押すと、ファイル選択画面が表示されます。

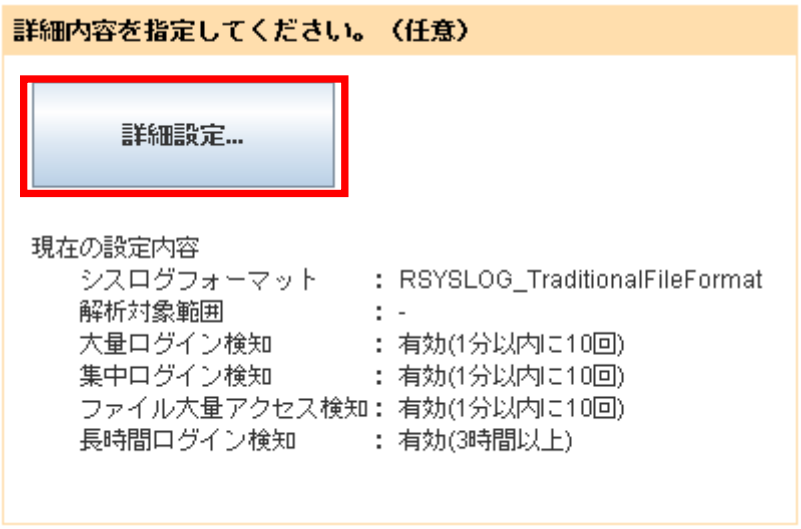


3.3.3. 解析結果出力の設定

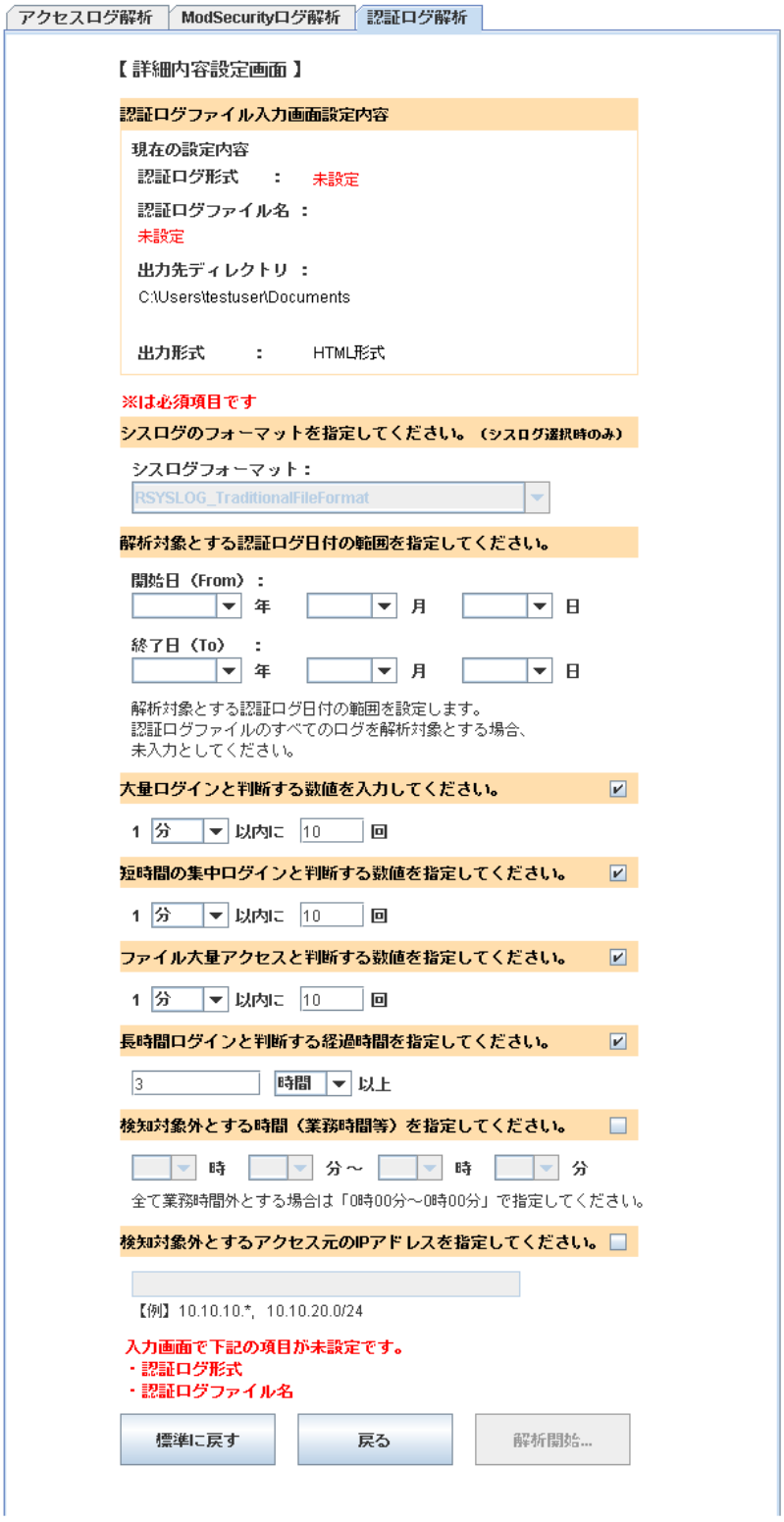
「3.1.3 解析結果出力の設定」を参照して下さい。

3.3.4. 詳細設定

詳細設定では、検出項目の有効/無効、項目ごとの閾値の設定、解析対象とする日付の範囲を設定できます。

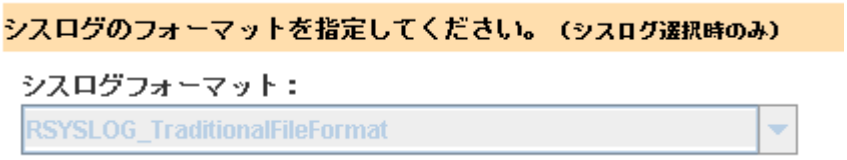


「詳細設定」ボタンを押した場合、詳細内容設定画面が表示されます。


アクセスログ解析
ModSecurityログ解析
認証ログ解析
【詳細内容設定画面】
認証ログファイル入力画面設定内容
現在の設定内容
認証ログ形式 ： 未設定
認証ログファイル名 ：
未設定
出力先ディレクトリ ：
C:\Users\testuser\Documents
出力形式 ： HTML形式
※は必須項目です
シスログのフォーマットを指定してください。（シスログ選択時のみ）
シスログフォーマット：
RSYSLOG_TraditionalFileFormat
解析対象とする認証ログ日付の範囲を指定してください。
開始日（From）：
年 月 日
終了日（To）：
年 月 日
解析対象とする認証ログ日付の範囲を設定します。
認証ログファイルのすべてのログを解析対象とする場合、
未入力としてください。
大量ログインと判断する数値を入力してください。
1 分 以内に 10 回
短時間の集中ログインと判断する数値を指定してください。
1 分 以内に 10 回
ファイル大量アクセスと判断する数値を指定してください。
1 分 以内に 10 回
長時間ログインと判断する経過時間を指定してください。
3 時間 以上
検知対象外とする時間（業務時間等）を指定してください。
時 分～ 時 分
全て業務時間外とする場合は「0時00分～0時00分」で指定してください。
検知対象外とするアクセス元のIPアドレスを指定してください。
【例】10.10.10.*, 10.10.20.0/24
入力画面で下記の項目が未設定です。
・認証ログ形式
・認証ログファイル名
標準に戻す
戻る
解析開始...

（1） シスログフォーマット設定

syslog の解析を行う場合にフォーマットを指定します。syslog 以外の場合は指定できません。



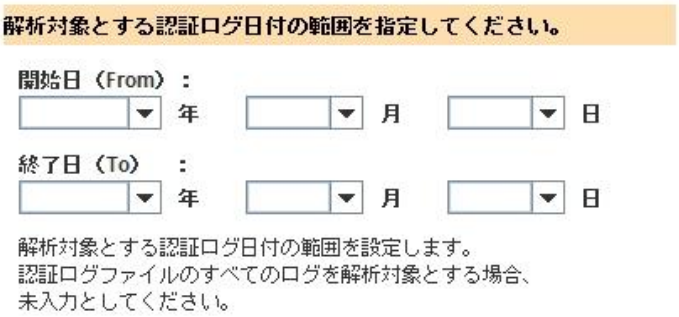
選択可能な形式は以下の通りです。

・RSYSLOG_TraditionalFileFormat

・RSYSLOG_FileFormat

（2） 日付範囲選択

解析対象の認証ログファイルの日付範囲を指定します。

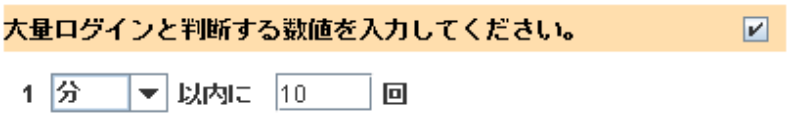


開始日のみ指定した場合、その日からのアクセスログを検出対象とします。
終了日のみ指定した場合、その日までのアクセスログを検出対象とします。
日付を指定しない場合、すべてのアクセスログを検出対象とします。

※シスログフォーマットが RSYSLOG_TraditionalFileFormat の場合、ログに年情報が含まれないため、開始年/終了年の指定は無視され、月日の指定のみが有効となります

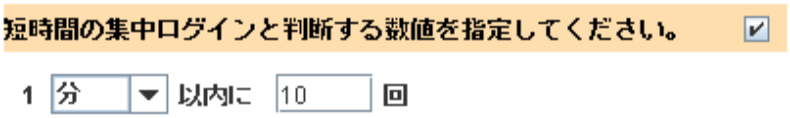
（３） 大量ログインの閾値

同一ユーザから一定時間内に大量のログインがあったと判断する閾値を設定します。単位時間(分、時間、日)をドロップダウンで選択し、回数をテキストボックスで入力します。チェックボックスで本項目の有効／無効を選択できます。無効にした場合、本項目の解析は行われません。



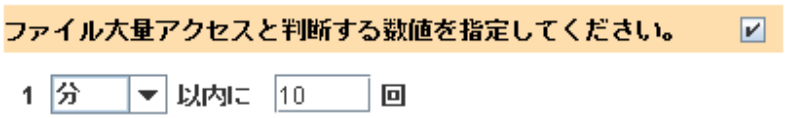
（４） 短時間の集中ログインの閾値

短時間に集中してログイン要求があったと判断する閾値を設定します。単位時間(分、時間、日)をドロップダウンで選択し、回数をテキストボックスで入力します。チェックボックスで本項目の有効／無効を選択できます。無効にした場合、本項目の解析は行われません。



（５） ファイル大量アクセスの閾値

同一ファイルに大量アクセスがあったと判断する閾値を設定します。単位時間(分、時間、日)をドロップダウンで選択し、回数をテキストボックスで入力します。チェックボックスで本設定の有効／無効を選択できます。無効にした場合、本項目の解析は行われません。

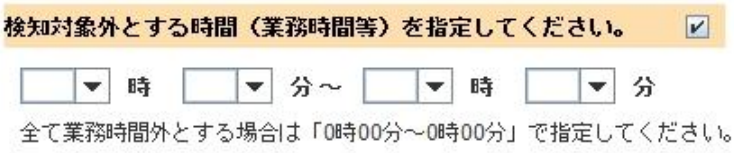


（６） 長時間ログインの閾値

長時間ログイン状態であると判断する閾値を設定します。数値をテキストボックスで入力し、単位時間(分、時間、日)をドロップダウンで選択します。チェックボックスで本設定の有効／無効を選択できます。無効にした場合、本項目の解析は行われません。

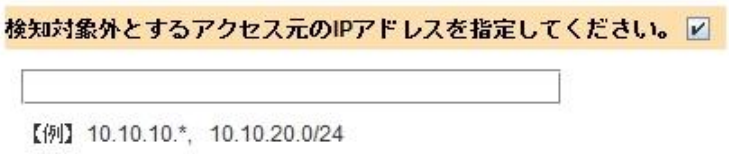
（７） 検知対象外時間

検知対象外の時間帯（業務時間等）を指定します。このルールを有効にした場合、ここで指定した時間に含まれないログが全て検知されます。チェックボックスで本設定の有効／無効を選択できます。無効にした場合、本項目の解析は行われません。



（８） 検知対象外 IP アドレス

検知対象外のアクセス元 IP アドレスを指定します。カンマ区切りでの複数指定、*（アスタリスク）によるワイルドカード指定、/（スラッシュ）によるサブネットマスク指定が可能です。このルールを有効にした場合、ここで指定した以外のアクセス元からのログが全て検知されます。チェックボックスで本設定の有効／無効を選択できます。無効にした場合、本項目の解析は行われません。



（９） 設定解除と画面遷移

「標準に戻す」ボタンを押すと、初期表示の状態に戻します。初期値について、下記のとおりです。

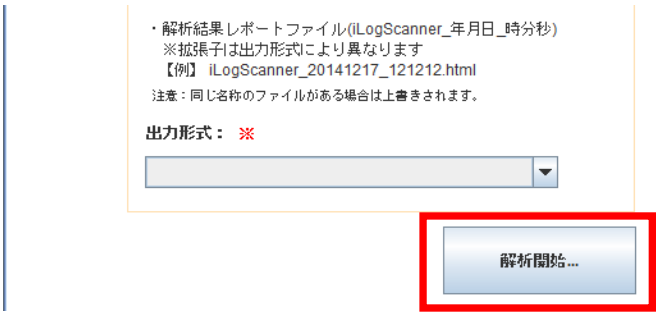
シスログフォーマット：RSYSLOG_TraditionalFileFormat
開始日：空白
終了日：空白
大量ログインの閾値：有効（1 分以内に 10 回）
短時間の集中ログインの閾値：有効（1 分以内に 10 回）
ファイル大量アクセスの閾値：有効（1 分以内に 10 回）
長時間ログインの閾値：有効（3 時間以上）
検知対象外時間：無効
検知対象外 IP アドレス：無効

「戻る」ボタンを押すと、認証ログ入力画面へ遷移します。

「解析開始」ボタンを押すと、設定の適当性をチェックし、アクセスログ解析が開始されます。正しく設定されていない場合、エラーメッセージを表示し、その後解析は行われません。

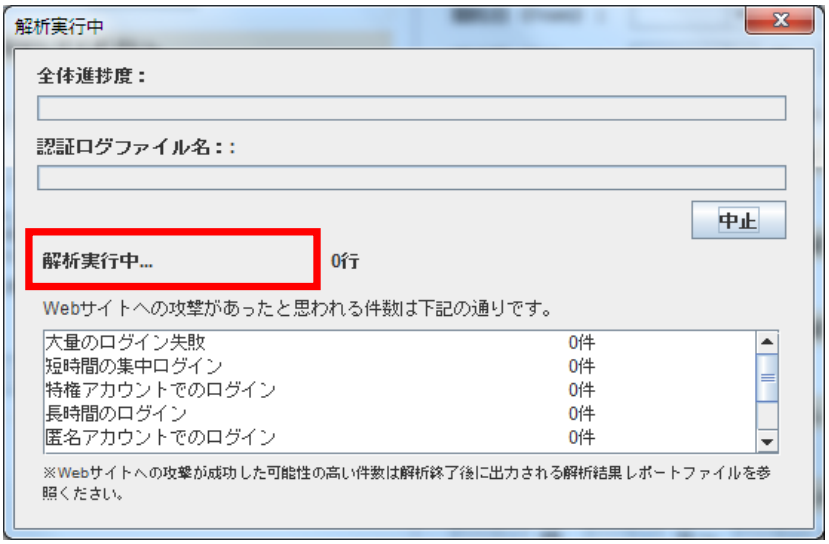
3.3.5. 解析開始

認証ログ形式、解析対象ログファイル、出力形式、出力先ディレクトリをそれぞれ設定後、解析開始ボタンを押すと解析が開始されます。認証ログ形式、解析対象ログファイル、出力形式、出力先ディレクトリが全て設定されていない場合、解析は行われません。

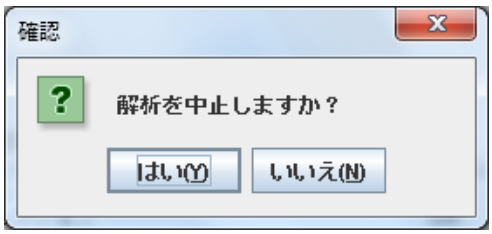


解析が開始されると、解析実行中画面は以下の通りに表示します。

認証ログファイル解析中

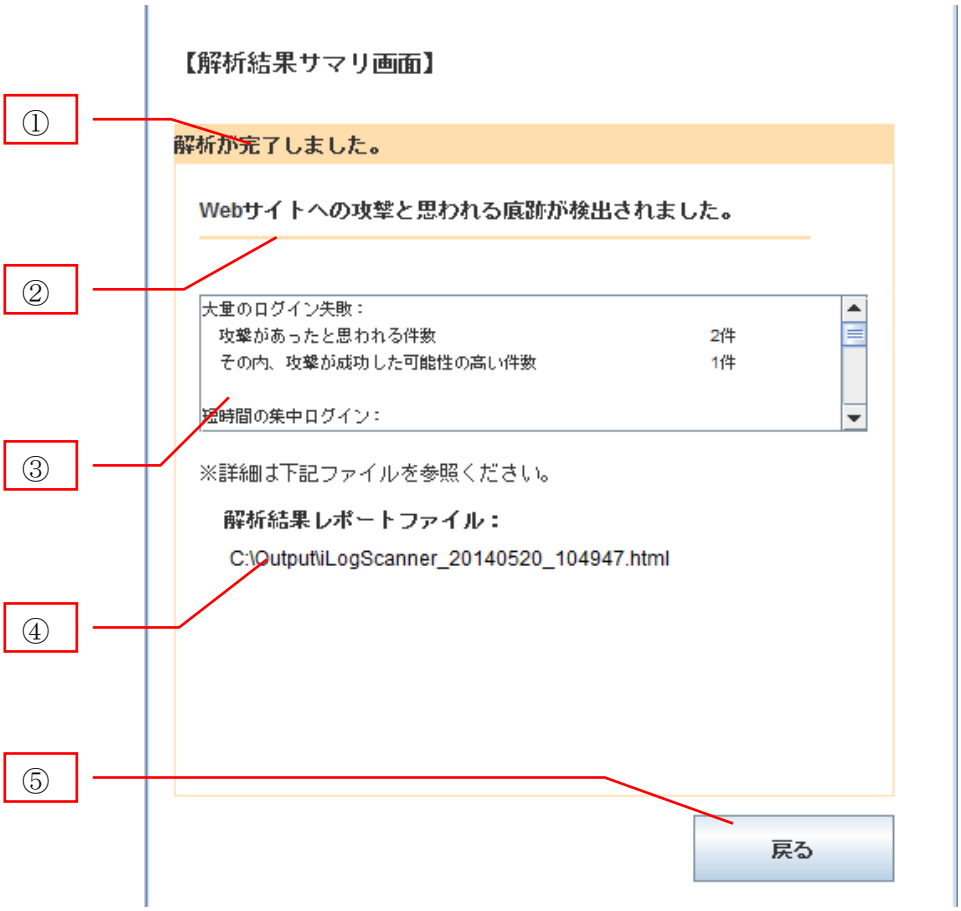


中止ボタンを押した場合、確認ダイアログが表示されます。確認ダイアログの「はい」を選択した場合、処理を中止しその時点での解析結果が出力されます。「いいえ」を選択した場合、解析実行中画面に戻ります。



3.3.6. 解析終了

認証ログ解析が終了した後、解析結果レポートファイルを作成し、結果画面が表示されます。



解析結果サマリ画面の①は終了メッセージ(完了/中止)が表示されます。②は攻撃痕跡の有無を示すメッセージが表示されます。③は検出対象項目と検出数が表示されます。④は解析結果レポートファイルのパス付ファイル名が表示されます。解析結果レポートファイルは、解析実行時に指定したディレクトリに出力されます。⑤の「戻る」ボタンをクリックすると認証ログ解析画面に戻ります。

認証ログ解析を中止した場合やエラーにより解析中止となった場合は、その時点までの解析結果を出力します。

3.3.7. 解析結果レポート

解析結果レポートは、認証ログ解析終了後、解析前に指定した出力先ディレクトリに出力されます。HTML 形式で出力した場合の例を以下に示します。

解析結果レポートには、以下の項目が出力されます。

・解析結果

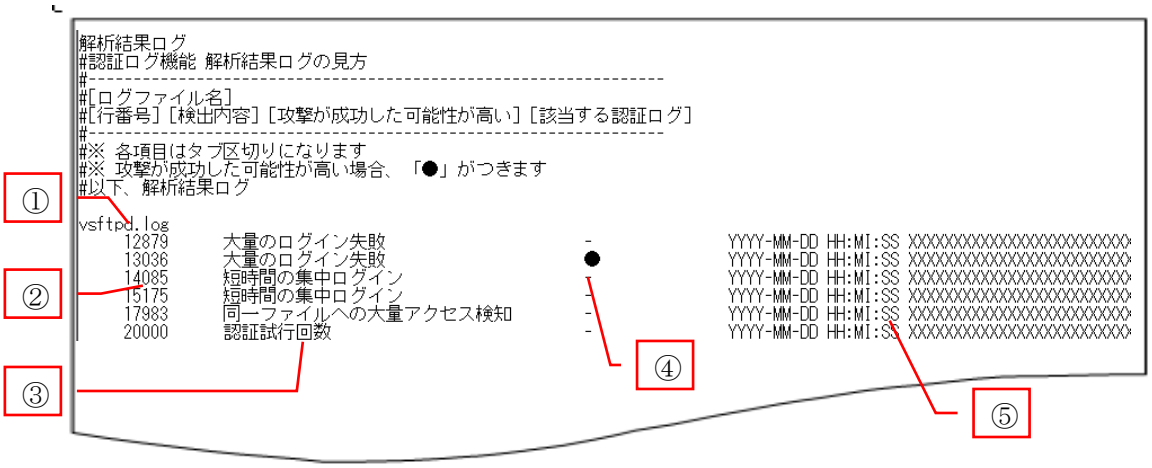
終了ステータス(完了/中止)、解析日時、解析対象ファイル、解析指定日付、解析対象日付、検出数が表示されます。

・検出した内容の説明と対策

iLogScanner が検出対象としている項目についての説明が表示されます。

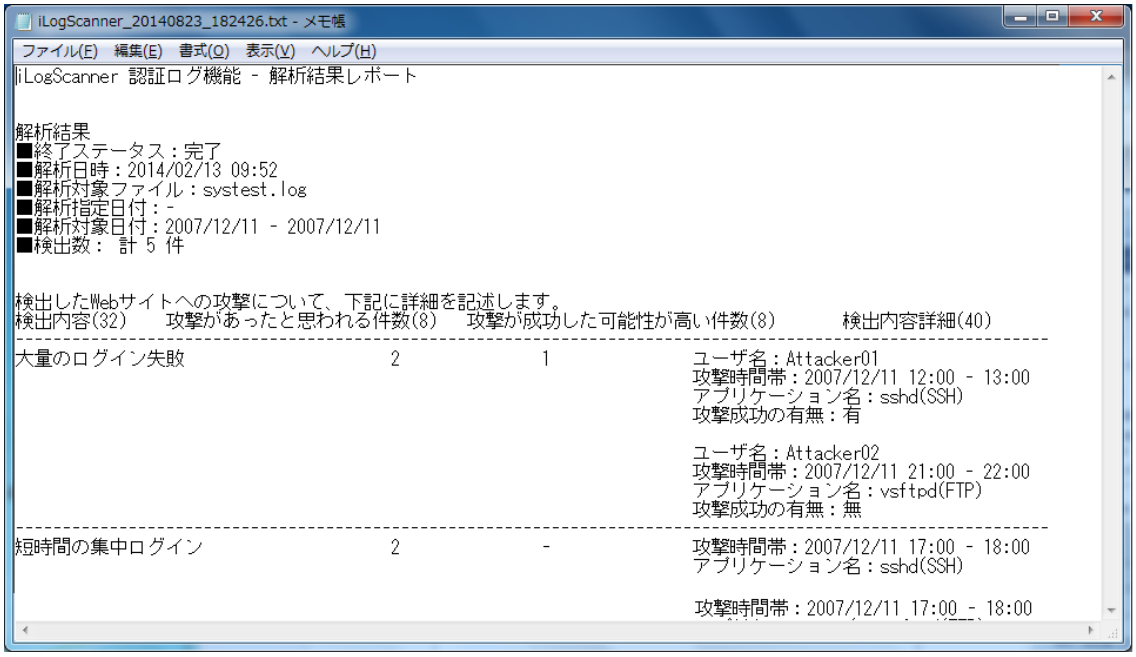
・解析結果ログ

攻撃の痕跡を検出したログの内容を出力します。解析結果ログファイルの形式は以下のとおりです。



①は攻撃痕跡を検出したファイル名が出力されます。②は検出したアクセスログの行番号が出力されます。③は検出した脆弱性項目名が出力されます。④は攻撃された可能性が高い場合に「●」が出力されます。⑤は検出されたアクセスログが出力されます。

TEXT 形式で出力した場合の例を以下に示します。出力される項目は HTML 形式と同一です。



XML 形式のレポートについては付録を参照してください。

4. トラブルシュート

iLogScanner の動作に関する不明点は、下記 URL の FAQ を参照してください。

https://www.ipa.go.jp/security/vuln/iLogScanner/app/faq.html#top

5. 付録　XML 形式の解析結果レポートファイル

iLogScanner が出力するレポートを攻撃検知のトリガーとして、外部のプログラムが自動的に取込むことができるように XML 形式による出力をサポートします。一般的に XML 文章は、テキストエディタやビューアによる閲覧には適していないため、利用者が視覚的に解析結果を確認するにはスタイリングされた HTML 形式や TEXT 形式での出力を推奨します。

5.1. XML スキーマ定義方針

HTML 形式や TEXT 形式との差異はフォーマットの違いだけで、出力する内容は同じとします。

レポートの種類別（アクセスログ解析、ModSecurity ログ解析、認証ログ解析）にスキーマを定義せず、レポート全体を 1 つの XML スキーマで定義します。要素がどのレポート種別で有効であるかは各種要素の定義にて記載します。

5.2. XML スキーマ定義

XML 宣言

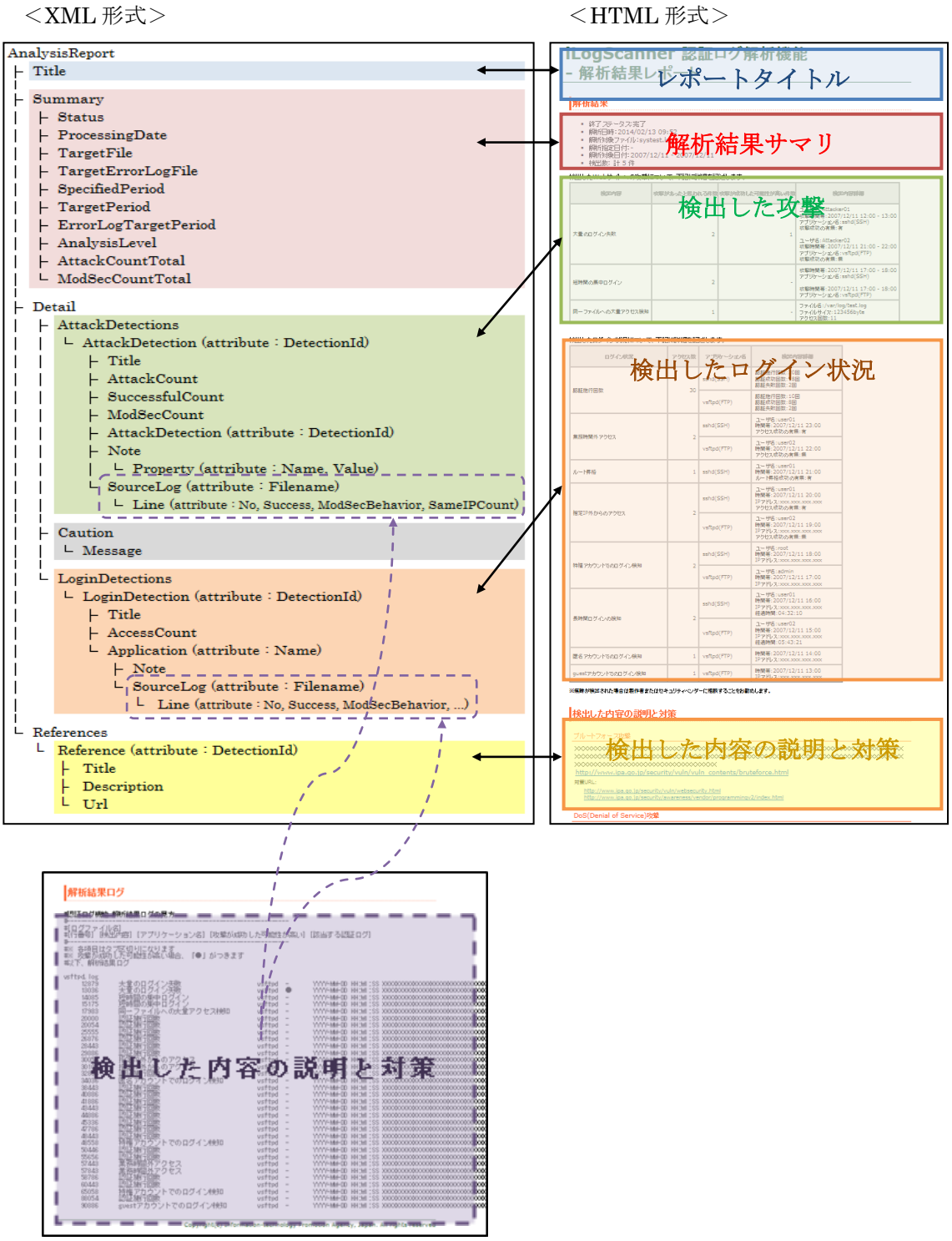
書式	<?xml version="1.0" encoding="shift_jis"?>

属性	値	備考
version	1.0	XML を生成するプログラムは、XML 1.1 特有の機能が必要とされない限り、XML 1.0 を生成する事が望ましい※
encoding	shift_jis	

※ http://www.w3.org/TR/xml11/#proc-types

5.3. XML 文書構造の全体像

・解析結果レポートの XML スキーマ全体像と HTML 形式との関連を以下に示します。



5.4. 各種要素

① ルート要素

要素	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析（統計）	認証ログ解析
AnalysisReport	解析結果レポートのルート要素	1	○	○	○	○

② AnalysisReport 直下の要素

要素	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析（統計）	認証ログ解析
Title	解析結果レポートのタイトル	1	○	○	○	○
Summary	解析結果のサマリ	1	○	○	○	○
Detail	解析結果の詳細	1	○	○	○	○
References	検出した内容の説明と対策一覧	1	○	○	○	○

③ Summary 直下の要素

要素	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析（統計）	認証ログ解析
Status	終了ステータス	1	○	○	○	○
ProcessingDate	解析日時	1	○	○	○	○
TargetFile	解析対象ファイル	0 or 1	○	○	-	○
TargetErrorLogFile	解析対象エラーログファイル	0 or 1	-	○	○	-
SpecifiedPeriod	解析指定日付	1	○	○	○	○
TargetPeriod	解析対象日付	0 or 1	○	○	-	○
ErrorLogTargetPeriod	エラーログの解析対象日付	0 or 1	-	○	○	-
AnalysisLevel	解析レベル	1	○	○	-	-
AttackCountTotal	攻撃検出数の合計	1	○	○	-	○
ModSecCountTotal	ModSecurity で検出・遮断した件数の合計	1	-	○	○	-

④ Detail 直下の要素

要素	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析（統計）	認証ログ解析
AttackDetections	検出した攻撃一覧	1	○	○	○	○
Caution	警告情報	0 or 1	○	○	-	-
LoginDetections	検出したログイン状況一覧	0 or 1	-	-	-	○

⑤ AttackDetections 直下の要素

要素	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析（統計）	認証ログ解析
AttackDetection	検出した攻撃	1 以上	○	○	○	○

⑥ AttackDetection 要素

・属性

属性	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析（統計）	認証ログ解析
DetectionId	検出内容の対応コード	1	○	○	○	○

※検出内容の対応コードの一覧は「7.5 検出内容の対応コード」を参照

・直下の要素

要素	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析（統計）	認証ログ解析
Title	検出内容のタイトル（シグネチャの名称）	1	○	○	○	○
AttackCount	攻撃があったと思われる件数	0 or 1	○	○	-	○
ModSecCount	ModSecurity で検出・遮断した件数	0 or 1	○	○	○	○
SuccessfulCount	攻撃が成功した可能性が高い件数	0 or 1	-	○	-	-
Note	検出内容詳細	0 以上	-	-	-	○
AttackDetection	検出した攻撃に分類される内訳要素。再帰構造。 例.「Web サーバの設定不備を狙った攻撃の可能性」 AttackDetection は「PUT メソッドの設定不備」AttackDetection を持つ。	0 以上	○	○	○	-
SourceLog	攻撃と判断したログの一覧（ファイルごとに 1 要素）	0 以上	○	○	○	○

⑦Note 直下の要素

要素	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析(統計)	認証ログ解析
Property	詳細情報の細目	0 以上	-	-	-	○

⑧Property 要素の属性

属性	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析(統計)	認証ログ解析
Name	細目の名称	1	-	-	-	○
Value	細目の値	1	-	-	-	○

⑨SourceLog 要素

・属性

属性	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析(統計)	認証ログ解析
FileName	ログファイル名	1	○	○	○	○

・直下の要素

要素	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析(統計)	認証ログ解析
Line	1 行分のログ	1 以上	○	○	○	○

⑩Line 要素の属性

属性	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析（統計）	認証ログ解析
No	行番号	1	○	○	○	○
Success	攻撃が成功した可能性が高い場合、true	0 or 1	○	○	○	○
ModSecBehavior	攻撃に対する ModSecurity の振る舞い "denied" "captured" "deficiency"	0 or 1	－	○	－	－
SameIPCount	同一 IP アドレスからの攻撃検出数	0 or 1	－	○	－	－
SignatureCode	シグネチャコード	0 or 1	○	○	－	－

※Line のテキスト要素には該当するログの 1 レコードのデータが出力される

⑪Caution 直下の要素

要素	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析（統計）	認証ログ解析
Message	警告メッセージ	1 以上	○	○	－	－

⑫LoginDetections 直下の要素

要素	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析（統計）	認証ログ解析
LoginDetection	検出したログイン状況	1 以上	-	-	-	○

⑬LoginDetection 要素

・属性

属性	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析（統計）	認証ログ解析
DetectionId	検出内容の対応コード	1	-	-	-	○

※検出内容の対応コードの一覧は「5.5 検出内容の対応コード」を参照

・直下の要素

要素	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析（統計）	認証ログ解析
Title	検出内容のタイトル（シグネチャの名称）	1	-	-	-	○
AccessCount	アクセス数	1	-	-	-	○
Application	検出したアプリケーション	1	-	-	-	○

⑭Application 要素

・属性

属性	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析（統計）	認証ログ解析
Name	アプリケーション名	1	-	-	-	○

・直下の要素

要素	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析（統計）	認証ログ解析
Note	検出内容詳細	1 以上	-	-	-	○
SourceLog	ログイン状況にカウントしたログの一覧 （ファイルごとに 1 要素）	0 以上	-	-	-	○

⑮References 直下の要素

要素	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析(統計)	認証ログ解析
Reference	検出した内容の説明と対策	1 以上	○	○	○	○

⑯Reference 要素

・属性

属性	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析(統計)	認証ログ解析
DetectionId	検出内容の対応コード 複数ある場合は、カンマ区切り	1	○	○	○	○

※検出内容の対応コードの一覧は「5.5 検出内容の対応コード」を参照

・直下の要素

要素	意味・内容	出現回数	アクセスログ解析	ModSecログ解析	ModSecログ解析(統計)	認証ログ解析
Title	検出内容のタイトル(シグネチャの名称)	1	○	○	○	○
Description	説明文	1	○	○	○	○
Url	対策 URL	0 以上	○	○	○	○

5.5. 検出内容の対応コード（DetectionId）

検出内容は日本語の文章になっているため、プログラムが判別しやすいよう、検出内容に対し一意のコードを付与します。コードの一覧は下記の通りです。

レポート分類	検出内容	コード	備考
解析結果レポート(アクセスログ解析機能、ModSecurity ログ解析機能)	SQL インジェクション	WEB_ATK_SQL	
	OS コマンドインジェクション	WEB_ATK_CMD	
	ディレクトリトラバーサル	WEB_ATK_DT	
	クロスサイトスクリプティング	WEB_ATK_XSS	
	その他	WEB_ATK_OTHER	
	同一 IP アドレスからの攻撃の可能性	WEB_ATK_DETAIL_IP	「詳細」時のみ
	アクセスログに記録されない SQL インジェクションの可能性	WEB_ATK_DETAIL_SQL	「詳細」時のみ
	Web サーバの設定不備を狙った攻撃の可能性	WEB_ATK_DETAIL_SRV	「詳細」時のみ
	PUT メソッドの設定不備	WEB_ATK_DETAIL_SRV_PUT	「詳細」時のみ
	FrontPage Server Extensions の設定不備	WEB_ATK_DETAIL_SRV_FP	「詳細」時のみ
	Tomcat の設定不備	WEB_ATK_DETAIL_SRV_TOM	「詳細」時のみ
	上記以外の分類（ModSecurity）	WEB_ATK_MDSC	ModSec のみ
統計情報レポート（ModSecurity ログ解析機能）	WEB_ATTACK/SQL_INJECTION	MDSC_ATK_SQL	
	WEB_ATTACK/COMMAND_INJECTION	MDSC_ATK_CMD	
	WEB_ATTACK/FILE_INJECTION	MDSC_ATK_DT	
	WEB_ATTACK/XSS	MDSC_ATK_XSS	
	WEB_ATTACK/UPDF_XSS	MDSC_ATK_UPDF_XSS	

分析結果レポート解析 （認証ログ解析機能）	攻撃の兆候の確認		
	大量のログイン失敗	AUTH_ATK_LOGIN	
	短時間の集中ログイン	AUTH_ATK_CONCENT	
	同一ファイルへの大量アクセス検知	AUTH_ATK_FILE	
	ログイン状況の確認		
	認証試行回数	AUTH_STS_LOGIN	
	業務時間外アクセス	AUTH_STS_OFFWORK	
	ルート昇格	AUTH_STS_SU	
	指定 IP 外からのアクセス	AUTH_STS_EXIP	
	特権アカウントでのログイン検知	AUTH_STS_ADMIN	
	長時間ログインの検知	AUTH_STS_LONGTIME	
	匿名アカウントでのログイン検知	AUTH_STS_ANONYMOUS	
	ゲストアカウントでのログイン検知	AUTH_STS_GUEST	